Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 30 *XXX*
Number 1

Article 6

2019

The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age of Alexa

Lauren Bass
Fordham University School of Law, lbass4@law.fordham.edu

The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age of Alexa

Cover Page Footnote

J.D. Candidate, Fordham University School of Law, 2020. B.A., Brown University. I wish to acknowledge the invaluable contributions, insightful comments, and steadfast encouragement of IPLJ Senior Writing & Research Editor, Elliot Fink, and Professor Olivier Sylvain. I would also like to thank my family for their unwavering support— especially my mother for being my mentor, my sounding board, and my first writing teacher.

The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age of Alexa

Lauren Bass*

In today's interconnected, internet-dependent, global information economy, consumers willingly, but often unwittingly, divulge to tech companies their personal and private data—frequently with little regard for its safekeeping or intended future use.

Enter Alexa, Amazon's voice-activated, natural-language processing digital smart assistant. A sophisticated artificial intelligence ("AI"), Alexa insinuates itself into a user's personal sphere, learns from and adapts to the surrounding environment, siphons personal information and data, and ultimately produces for the user a perfectly tailored, concierge experience. Convenience is the product. Data privacy is the cost.

Over one half of American consumers own an Alexa-enabled device or other AI-powered digital smart assistant. This rapid adoption of AI technology has created the potential for an untenable and unsustainable surveillance state in which private data brokers such as Amazon can control the flow of information and hold hostage the individual consumer.

The existing U.S. legal framework—a sectoral regime heavily dependent upon the principals of "Notice and Choice," under the ineffectual oversight of the Federal Trade Commission—is ill-equipped to deal with the privacy issues presented by the AI-based

* J.D. Candidate, Fordham University School of Law, 2020. B.A., Brown University. I wish to acknowledge the invaluable contributions, insightful comments, and steadfast encouragement of IPLJ Senior Writing & Research Editor, Elliot Fink, and Professor Olivier Sylvain. I would also like to thank my family for their unwavering support—especially my mother for being my mentor, my sounding board, and my first writing teacher.

data collection of smart assistants. The time for comprehensive federal data privacy reform is now. The states should not shoulder this burden. Instead, Congress must act to establish a uniform system of rules that will federally regulate the collection and retention practices of data brokers and safeguard the autonomy and data privacy of the individual.

INTRODUCTION

Home Surveillance—the term conjures images of conspicuously placed cameras along the perimeter of one's domicile, judiciously employed for security purposes to monitor and prevent access from outside intruders or bad actors. Today, however, the term *home surveillance* more aptly describes the technology employed *inside* a modern "smart" home.[1] Marketed as a gadget of convenience, the voice-enabled smart assistant—a recent addition to the Internet of Things ("IoT")[2]—purports to aid daily life, automating simple and mundane tasks such as regulating the thermostat[3] or ordering a pizza.[4] Beneath the sleek futuristic exterior, however, a smart

---

1 *See* Anick Jesdanun, *Advances in Smart Home Tech Raise Privacy Concerns*, CLAIMS J. (Jan. 8, 2019), https://www.claimsjournal.com/news/national/2019/01/08/288630.htm [https://perma.cc/78LS-YCM5] (quoting Jeff Chester, executive director for the Center for Digital Democracy, as saying, "It's decentralized surveillance . . . . We're living in a world where we're tethered to some online service stealthily gathering our information.").

2 The Internet of Things ("IoT") refers to "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." *See Internet of Things*, GARTNER.COM: IT GLOSSARY, https://www.gartner.com/it-glossary/internet-of-things [https://perma.cc/6EQ3-AG4D]. For a more detailed explanation of the history and evolution of IoT, see Knud Lasse Luth, *Why the Internet of Things Is Called Internet of Things: Definition, History, Disambiguation*, IOT ANALYTICS (Dec. 19, 2014), https://iot-analytics.com/internet-of-things-definition/ [https://perma.cc/8LY9-9DYV]. This Note focuses solely on Alexa-enabled AI digital assistants, a small subsection of IoT.

3 *See, e.g.*, *Nest Learning Thermostat Overview*, NEST, https://nest.com/thermostats/nest-learning-thermostat/overview/ [https://perma.cc/UAW3-TBGF].

4 *See* Eugene Kim, *The Inside Story of How Amazon Created Echo, the Next Billion-Dollar Business No One Saw Coming*, BUS. INSIDER (Apr. 2, 2016, 12:01 PM),

assistant is little more than surveillance equipment—cameras, microphones, and AI learning centers—embedded into the home under the guise of "the next big thing in computing."[5] This new form of constant surveillance no longer aims to keep *out*, but rather to draw *in*—engaging and ensnaring consumers into allowing the mavericks of Silicon Valley to indiscriminately collect, mine, store, and analyze endless amounts of data willingly offered by their subjects, all under the façade of convenience.[6]

This rapid adoption of AI technology, substantially in the form of voice-enabled smart assistants like Amazon's Alexa, has created the potential for a monopolistic surveillance state in which Amazon and other private data brokers dominate, controlling the flow of information, wielding immense market power, and essentially holding the individual consumer hostage.[7] Afraid of stifling innovation and dampening the progress of capitalism,[8] Congress, to date, has maintained an arms-length approach to regulating both Silicon Valley and its Big Data practices. However, as AI voice-technology continues to infiltrate and embed itself into the daily fabric, the prevailing U.S. legal framework—a sectoral regime heavily reliant upon the fair information principles of Notice and Choice[9] coupled with limited Federal Trade Commission ("FTC") oversight—is ill-equipped to efficiently or effectively regulate the predatory privacy

---

https://www.businessinsider.com/the-inside-story-of-how-amazon-created-echo-2016-4 [https://perma.cc/Y2T3-ESNX].

5 Elad Natanson, *Artificial Intelligence Smart Assistants: The Next Big Thing in Computing?*, FORBES (June 22, 2017, 7:42 AM), https://www.forbes.com/sites/eladnatanson/2017/06/22/artificial-intelligence-smart-assistants-the-next-big-thing-in-computing/#19d371534252 [https://perma.cc/A9U6-HV8A].

6 *See* Jesdanun, *supra* note 1; *see also* John Paul Titlow, *Smart Homes: Our Next Digital Privacy Nightmare*, READWRITE (Mar. 18, 2013), https://readwrite.com/2013/03/18/smart-homes-our-next-digital-privacy-nightmare/ [https://perma.cc/P5N4-5FDW].

7 *See* Katharine Schwab, *Amazon Could Soon Force You to Go on a Diet, According to One Futurist*, FAST CO. (Mar. 21, 2019), https://www.fastcompany.com/90322180/amazon-could-soon-force-you-to-go-on-a-diet-according-to-one-futurist [https://perma.cc/7SPT-46AK].

8 *See* Omar Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 63 (2012) (warning that a "regulatory backlash" could dampen the data economy and stifle innovation).

9 *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 80–83 (2018).

procedures of data-hungry tech companies, leaving consumers prey to abuses and violations in the collection, storage, and manipulation of their personal information.[10]

This Note argues that the time for comprehensive federal legislative privacy reform of the tech sector and its voracious data consumption practice is now. Using Amazon's voice-enabled AI, Alexa, as an illustrative example, this Note identifies key data privacy[11] issues raised by the rapid expansion and embrace of voice-enabled smart assistants, interrogates the effectiveness of the current legal privacy paradigms in protecting consumer privacy, and

---

[10] For the purposes of this Note, "personal information" will encapsulate both personally identifiable information ("PII") (see definition below) and non-PII, as advances in de-anonymization techniques have blurred the lines such that even non-PII may be easily used to identify an individual. *See* Kelsey Campbell-Dollaghan, *Sorry, Your Data Can Still Be Identified Even If It's Anonymized*, FAST COMPANY (Dec. 10, 2018), https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized [https://perma.cc/ZT53-7VNX]. PII is defined as:

> [A]ny information about an individual . . . including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual . . . .

ERIKA MCCALLISTER, TIM GRANCE & KAREN SCARFONE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800–122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) 2–1 (Apr. 2010) (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-08-536, PRIVACY: ALTERNATIVES EXIST FOR ENHANCING PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION 1 n.1 (2008). The National Institute of Standards and Technology ("NIST") explains:

> To *distinguish* an individual is to identify that individual . . . . To *trace* an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status . . . . *Linked* information is information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual.

Id.

[11] Data privacy, also synonymous with "informational privacy," is defined as "the ability to determine for yourself when and how others may collect and use your information." Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms and Consent*, 14 J. HIGH TECH. L. 370, 373 (2014). Note that data privacy differs from data protection, which deals with the securing of one's data against unauthorized access. The former is a legal issue, while the latter a technical one. *See* Rick Robinson, *Data Privacy vs. Data Protection*, IPSWITCH (Jan. 29, 2018), https://blog.ipswitch.com/data-privacy-vs-data-protection [https://perma.cc/5LPY-KMH6].

investigates potential solutions for the future. Part I examines the history and conception of personal privacy in Anglo-American law, as well as the threats posed by the expansion of AI and Big Data as embodied by Amazon's virtual smart assistant, Alexa. Part II exposes the fundamental differences between the privacy models implemented by the United States and the European Union ("EU"), explains the origins of the existing U.S. privacy paradigm, and queries that paradigm's ability to adequately regulate the private sector or protect individuals from privacy threats posed by rapidly advancing and unregulated AI technology. Part III explores the ways in which the law permits widespread unchecked collection of personal data by AI smart assistants and analyzes the limitations that the current operating framework presents. Part IV eyes the future and proposes reforms to the existing data privacy regime.

I. OVERVIEW

A. Anglo-American Conceptions of Privacy

The concepts of privacy and the protection of the individual against outside intrusive forces are fundamental tenets underlying much of Anglo-American jurisprudence.[12] The doctrines permeate property and tort law, under which the right to exclude has become one of the "most essential sticks" in an individual's "bundle of rights."[13] The principles are embedded in the U.S. Constitution in the First Amendment (which protects the privacy of one's personal beliefs),[14] the Third Amendment (which prohibits the mandatory quartering of soldiers in one's home),[15] the Fourth Amendment (which secures a "right of the people" against unwarranted and violative government intrusion upon "persons," "houses" and

---

[12] For a more detailed explanation of the origin of the maxim and its impact on Anglo-American law, see Jonathan L. Hafetz, *"A Man's Home Is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries*, 8 WM. & MARY J. WOMEN & L. 175, 175 (2002).

[13] *See, e.g.*, Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979); Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 435 (1982); United States v. Craft, 535 U.S. 274, 283 (2002).

[14] *See* U.S. CONST. amend. I.

[15] *See id*. amend. III.

"effects"),[16] and the Fifth Amendment (which protects personal information and privacy by proscribing self-incrimination).[17] Eleven state constitutions echo the federal provisions and provide even further explicit protections for individuals and their privacy rights.[18] Although the courts have stopped short of specifically defining that one is entitled to a "right to privacy," they have repeatedly employed the Ninth and Fourteenth Amendments to recognize and protect an intrinsic interest in individual autonomy, which has helped to shield minors from the detriments of indecent speech,[19] permit adult possession of pornography,[20] and safeguard couples' sovereignty within the bedroom.[21]

In the late nineteenth century, following the advent of the instantaneous camera and portable audio recording devices, both of which had the potential to readily breach individual privacy as well

---

16 *See id*. amend. IV. Although helpful here as an illustrative example, in general, the Fourth Amendment and its protections of privacy fall outside the scope of this Note.

17 *See id*. amend. V.

18 *See* ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CAL. CONST. art. I, § 1 ("All people . . . have inalienable rights. Among these are . . . privacy."); FLA. CONST. art. I, § 12 ("The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated."); HAW. CONST. art. I, §§ 6–7 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest."); ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means."); LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy."); MONT. CONST. art. II § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); N.H. CONST. pt. 1, art. 2-b ("An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent."); S.C. CONST. art. I, § 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated . . . ."); WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.").

19 *See* Fed. Commc'ns Comm'n v. Pacifica Found., 438 U.S. 726, 731 (1978).

20 *See* Stanley v. Georgia, 394 U.S. 557, 565 (1969).

21 *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484 (1965); Lawrence v. Texas, 539 U.S. 558, 574 (2003).

as the sanctity of the home,[22] Samuel Warren and Louis Brandeis penned their seminal treatise,[23] which introduced the common law principle of an individual's right "to be let alone."[24] Drawing on the doctrine of property—specifically that of exclusion[25]—this inherent privacy right aimed to safeguard one's human dignity and individuality,[26] or, as Warren and Brandeis termed it, the "inviolate personality."[27] According to their theory, an individual possesses exclusive control over his "thoughts, sentiments, and emotions," or, in other words, his personal and private data.[28] Such "possessions," argued Warren and Brandeis, could not (and should not) be appropriated (or misappropriated) by another without the individual's express consent.[29]

Warren and Brandeis loathed the idea that the gossip journalists' cameras and recording machines could intrude in any way upon their seclusion.[30] These "mechanical devices," they warned, "threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[31] To counteract any such unsanctioned invasion of privacy, Warren and Brandeis contended, the injurious violation of privacy by technology—the surreptitious taking of photographs or audio recordings—must be recognized as legally cognizable harms,[32] which could be identified and subsequently remedied in common-law tort proceedings.[33]

---

22 *See* WALDMAN, *supra* note 9, at 16.

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

24 *Id.* at 195. While commonly attributed to Warren and Brandeis, Thomas M. Cooley originally coined the phrase, the right "to be let alone" a decade earlier in his 1879 treatise. *See* THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (1879).

25 Warren & Brandeis, *supra* note 23, at 216.

26 Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 991 (1964).

27 Warren & Brandeis, *supra* note 23, at 205, 211.

28 *Id.* at 198.

29 *See id.*

30 *See id.* at 195, 206; *see also* Robert Grace, *Warren & Brandeis: The Right to Curate an Identity*, PHOTOBOX GROUP SECURITY BLOG (Dec. 4, 2017), https://pbx-group-security.com/blog/2017/12/04/the-right-to-curate-an-identity/ [https://perma.cc/TZC8-4BYT].

31 Warren & Brandeis, *supra* note 23, at 195.

32 *See id.* at 206.

33 *See id.* at 211.

Warren and Brandeis's "natural right" proved influential upon the courts[34] and state legislatures.[35] However, it was the codification of their principals within tort law by William Prosser that solidified those theories as the dominant Anglo-American approach to privacy.[36] In the late 1960s, Prosser surveyed the litigation landscape and identified four civil rights of action under which to classify privacy tort suits: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity placing one in a false light; and (4) appropriation of one's likeness for the advantage of another.[37] Born as they were out of Warren and Brandeis's philosophies, Prosser's torts naturally borrowed from the same underlying principles. Each tort invoked the doctrines and language of trespass, exclusion, and theft, and framed the legal harm as one of unauthorized access: a right of the individual to protect his person and his home by keeping others out.[38]

Scholars have argued that Prosser's contextualization of a privacy doctrine within the consolidated torts has been a "mixed" blessing.[39] On the one hand, it has provided courts with a clear categorization for inflicted harm.[40] On the other, it has stunted the growth and evolution of privacy law by allowing courts to rely solely on an artificial taxonomy rather than on a broad and malleable conceptualization.[41] As Professors Neil M. Richards and Daniel J. Solove contend, "[b]efore Prosser, courts looked to Warren and Brandeis's article and examined whether particular harms fell under the very broad principle of the 'right to be let alone.' After Prosser, courts looked to whether a particular harm fit into one of Prosser's four categories."[42] The privacy harms threatening individuals today—namely Silicon Valley's unregulated collection, storage and manipulation of personal data via new technology such as AI smart

---

34 *See, e.g.*, Pavesich v. New England Life Ins. Co., 50 S.E. 68, 73–74 (Ga. 1905).

35 *See, e.g.*, N.Y. CIV. RIGHTS LAW § 51 (McKinney 2019).

36 RESTATEMENT (SECOND) OF TORTS §§ 652B–D (AM. LAW. INST. 1977).

37 *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

38 *See* WALDMAN, *supra* note 9, at 95.

39 *See generally* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).

40 *See id.* at 1915 (arguing that "[a]fter Prosser, courts looked to whether a particular harm fit into one of Prosser's four categories").

41 *See id*.

42 *Id.*

assistants—cannot be accurately confined to or remedied by Prosser's torts. Instead they require a broader conceptualization that can adjust to the changing technological landscape and the emerging harms. As a result, privacy torts have failed as a viable solution to privacy threats facing Americans today.

Privacy is also inherently normative. Therefore, social, economic, and even religious concerns have further influenced and shaped Anglo-American conceptions and perceptions of privacy. Take, for example, the biblical parable of the Garden of Eden. When coaxed by the serpent, Eve finally eats the apple from the Tree of Knowledge.[43] Upon acquiring "knowledge," she immediately has an innate sense that her "privacy" is being invaded by Adam's gaze, so she protects her right to privacy with a well-placed fig leaf.[44] Today's fig leaves take the forms of walls, doors, window dressings, and security surveillance systems. These physical barriers express an intrinsic sense of liberty and property—a need to protect one's interests in person and possessions. We exclude that which we fear; we include that which we trust.

A man's home is his castle, and he protects it as such.[45] When threats to the home manifest as physical intrusions, they are easy to identify and ward off. But what happens when the privacy veil of the home is pierced, and the evil that one has previously endeavored to *exclude* becomes that which one is now eager and willing to *include*?

B. Amazon's AI, Alexa

Enter Alexa, Amazon's voice-enabled, natural-language processing, digital AI assistant.[46] First introduced in 2014, Alexa is

---

43 *See Genesis* 3:6.

44 *See id.*

45 "That the house of every one [sic] is to him as his Castle . . . *domus sua cuique est tutissimum refugium*." SIR EDWARD COKE, SELECTED WRITINGS OF SIR EDWARD COKE, VOL. 1, at 137 (Steve Sheppard ed., 2003). *See also* Gary Martin, *The Meaning and Origin of the Expression: An Englishman's Home Is His Castle*, PHRASE FINDER, https://www.phrases.org.uk/meanings/an-englishmans-home-is-his-castle.html [https://perma.cc/W8ES-L2FC].

46 *See* Megan Trout, *Amazon—A Winning Strategy Continues with Alexa*, HARV. BUS. SCH.: DIGITAL INITIATIVE (Feb. 1, 2017), https://digit.hbs.org/submission/amazon-a-winning-strategy-continues-with-alexa/ [https://perma.cc/LJ4N-PGY5].

the central nervous system and brain that powers Echo, Amazon's sleek smart speaker.[47] Originally offered as a hands-free means by which to control one's music collection,[48] today's Alexa has evolved from a simple DJ[49] to a ubiquitous and trusted household presence tasked with the responsibility of unlocking the front door,[50] turning on the lights,[51] regulating the thermostat,[52] ordering dinner,[53] assisting the kids with their homework,[54] cleaning the house,[55] and, at the end of a long day, even helping one to drift off into a quiet slumber.[56]

Although colloquially, the terms Echo and Alexa are often used interchangeably, they actually represent two very different entities within the larger Amazon ecosystem. The former refers to the

---

47 *See* Christina Bonnington, *Amazon Alexa Is the Home Assistant You Never Knew You Needed*, DAILY DOT (Mar. 4, 2019, 11:40 AM), https://www.dailydot.com/debug/amazon-alexa/ [https://perma.cc/CGF2-VXMF].

48 *See* Matt Weinberger, *How Amazon's Echo Went from a Smart-Speaker to the Center of Your Home*, BUS. INSIDER (May 23, 2017, 6:08 PM), https://www.businessinsider.com/amazon-echo-and-alexa-history-from-speaker-to-smart-home-hub-2017-5 [https://perma.cc/63ZS-KBYD].

49 *See* Dan Moren, *How to Play Amazon Music Using Alexa*, TOM'S GUIDE (Nov. 28, 2018, 12:40 PM), https://www.tomsguide.com/us/alexa-amazon-music,review-4512.html [https://perma.cc/5X2X-D3LK].

50 *See* Leena Rao, *Amazon's Alexa Now Can Lock Your Front Door*, FORBES (July 28, 2016), http://fortune.com/2016/07/28/alexa-amazon-august-smart-lock/ [https://perma.cc/BLT3-22SJ]; *see also Control Your August Smart Lock with Amazon Alexa*, AUGUST, https://www.august.com/pages/alexa [https://perma.cc/ A786-9DF5].

51 *See* Lori Gil, *How to Control Your Lights with Amazon Echo*, IMORE (Nov. 13, 2018), https://www.imore.com/how-control-your-lights-amazon-echo [https://perma.cc/Q2H9-RU88].

52 *See* Jason Fitzpatrick, *How to Control Your Nest Learning Thermostat with Alexa*, HOW-TO GEEK (June 20, 2017, 4:53 PM), https://www.howtogeek.com/247553/how-to-control-your-nest-learning-thermostat-with-alexa/ [https://perma.cc/ETB8-MV2C].

53 *See* Chelsea Stone, *Amazon Alexa Can Now Help You Order Takeout*, SELF (Jan. 5, 2017), https://www.self.com/story/amazon-alexa-now-orders-takeout [https://perma.cc/2EHR-L2CZ].

54 *See* Tyler Lacoma, *6 Ways Alexa Can Help Kids with Their Homework*, DIGITAL TRENDS (Feb. 26, 2019, 1:33 PM), https://www.digitaltrends.com/home/6-ways-alexa-can-help-kids-with-their-homework/ [https://perma.cc/NGP2-C7DK].

55 *See* Alina Bradford, *How Alexa Can Help You Clean Your House*, CNET (Apr. 24, 2018, 6:00 AM), https://www.cnet.com/how-to/how-to-clean-your-house-with-alexa/ [https://perma.cc/3X79-DPWY].

56 *See* Victoria Hoff, *How I Hacked My Amazon Echo to Help Me Sleep Better*, BYRDIE (Jan. 27, 2017), https://www.byrdie.com/amazon-echo-sleep-tips [https://perma.cc/T2W6-TQQL].

physical hardware that consumers purchase—the smart speaker that sits atop a counter in the kitchen or a nightstand in the bedroom and functions as a portal to Amazon's remote cloud servers.[57] The latter refers to the disembodied voice that represents the human-AI interaction—an aural personification of the complex neural network[58] that engages each time a user interacts with Amazon's intricate AI technology.[59]

Amazon actively markets its line of Alexa-enabled devices as "your family's friend"[60]—technology designed to make "life easier" and "more fun."[61] Beneath the attractive Madison Avenue sales pitch, however, Alexa, as embodied in the Echo, is a Trojan horse—an intelligent surveillance and data collection system earning entrance into personal spaces such as the home or office under the guise of "next gen" concierge tech.[62] Equipped with microphones, digital cameras, computer learning centers, an unquenchable thirst for consumer data, and the infinite capacity to store collected information in the cloud,[63] these AI-powered smart-home assistants gain unfettered access to the most private areas of a user's life, both physically—stationed in the living room, the kitchen, the dining

---

57 *See* Marie Black, *What Is Amazon Echo? A Complete Guide*, TECH ADVISOR (June 10, 2019), https://www.techadvisor.co.uk/news/audio/amazon-echo-3584881/ [https://perma.cc/36LL-DRBS].

58 "A neural network is a type of machine learning which models itself after the human brain. This creates an artificial neural network that via an algorithm allows the computer to learn by incorporating new data . . . termed deep learning." Jonas DeMuro, *What Is a Neural Network?*, TECHRADAR (Aug. 11, 2018), https://www.techradar.com/news/what-is-a-neural-network [https://perma.cc/9BLD-U7QH].

59 Kate Crawford & Vladan Joler, *Anatomy of an AI System: The Amazon Echo as an Anatomical Map of Human Labor, Data, and Planetary Resources*, AI NOW INST. & SHARE LAB (Sept. 7, 2018), https://anatomyof.ai/ [https://perma.cc/3HM5-NB4C].

60 Chris Davies, *How Private Is Amazon Echo?,* SLASH GEAR (Nov. 7, 2014, 11:22 AM), https://www.slashgear.com/how-private-is-amazon-echo-07354486/ [https://perma.cc/Q4E6-569F].

61 *Alexa User Guide: Learn What Alexa Can Do*, AMAZON, https://amzn.to/2RkP9DA [https://perma.cc/TU5F-4R6S].

62 Shashank M, *Rise of the Smart Home Assistants*, MEDIUM (May 31, 2018), https://medium.com/@shanky101/rise-of-the-smart-home-assistants-e3fb7d3a9f58 [https://perma.cc/29AD-3ELM].

63 *See* Kim Wetzel, *What Is Alexa, and What Can Amazon's Virtual Assistant Do for You?*, DIGITAL TRENDS (Feb. 16, 2019, 7:25 AM), https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do [https://perma.cc/S5PL-HWAD].

room and even the bedroom[64]—and emotionally, as users willingly divulge personal and often confidential information.

Once inside a user's private sphere, Alexa remains ever vigilant and always listening.[65] Like Beyoncé, Alexa simply asks that you say her name[66] to call her to action.[67] Her functionality, however, is not self-contained within the hardware; Alexa and her intelligence exist wholly on Amazon's cloud servers. Therefore, all requests are recorded and transmitted to Amazon for processing.[68] To accomplish this, Alexa remains constantly tethered to the internet to allow

---

64 *See* Tom Warren, *Amazon's Echo Spot Is a Sneaky Way to Get a Camera into Your Bedroom*, VERGE (Sept. 28, 2017, 10:02 AM), https://www.theverge.com/2017/9/28/16378472/amazons-echo-spot-camera-in-your-bedroom [https://perma.cc/2M4B-7QSZ].

65 *See* Jenna Wortham, *How Alexa Fits into Amazon Prime's Directive*, N.Y. TIMES MAG. (Jan. 24, 2017), https://www.nytimes.com/2017/01/24/magazine/how-alexa-fits-into-amazons-prime-directive.html [https://perma.cc/VUQ3-ZE4U].

66 *See* DESTINY'S CHILD, *Say My Name*, *on* THE WRITING'S ON THE WALL (Columbia Records 1999).

67 *See* Grant Clauser, *What Is Alexa? What is the Amazon Echo, and Should You Get One?*, WIRECUTTER (Jan. 29, 2019), https://thewirecutter.com/reviews/what-is-alexa-what-is-the-amazon-echo-and-should-you-get-one/ [https://perma.cc/WF9G-JLQB].

68 *See id.* It should be noted that Amazon permits a user to delete recordings—or even the entire history—from its account. Such deletion of the file, however, does not necessarily guarantee complete deletion of the information contained within that file. Amazon is less than transparent as to whether deletion from a user's account also means deletion from Amazon's servers. *See* Conor Allison, *How to Delete Your Amazon Alexa Voice History*, AMBIENT (July 3, 2019), https://www.the-ambient.com/how-to/delete-voice-recordings-amazon-alexa-134 [https://perma.cc/VRF3-SKP5]; *see also* Alfred Ng, *Amazon Alexa Transcripts Live On, Even After You Delete Voice Records*, CNET (May 9, 2019, 7:40 AM), https://www.cnet.com/news/amazon-alexa-transcripts-live-on-even-after-you-delete-voice-records/ [https://perma.cc/V5KD-PERC]. It should be further noted that Amazon recently came under scrutiny for allowing recordings to be examined and studied by human engineers without user consent. *See* Matt Day, Giles Turner & Natalie Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019, 3:34 PM), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio [https://perma.cc/3BZ7-T4WX]. Since that scandal broke, Amazon has revised their policies to allow for users to opt-out of the human review system. *See* Matt Day, *Amazon Gives Option to Disable Human Review on Alexa*, BLOOMBERG (Aug. 2, 2019, 4:03 PM), https://www.bloomberg.com/news/articles/2019-08-02/amazon-gives-option-to-disable-human-review-of-alexa-recordings [https://perma.cc/D9FY-64R6].

data to flow freely back and forth from the connected home to Amazon's cloud and processing servers.[69]

Alexa's ability to learn from and adapt to her surroundings makes her attractive and unique to a user seeking a customized concierge experience.[70] It also makes her dangerous. Like Audrey II's insatiable appetite for blood in *Little Shop of Horrors,*[71] Alexa feeds on a constant diet of user data. The more data a user provides about her needs and desires, the better and more tailored the service that Alexa delivers,[72] and in turn, the more the user becomes enmeshed with and dependent upon Amazon's ecosystem.[73] A casual or occasional Alexa user might only provide Amazon with the minimum basic information required to operate the device, such as one's name or email. If a user wants to expand Alexa's functionality to facilitate in-app purchases or Amazon Prime home deliveries, the user might then provide Amazon with a credit card or banking information, a cell phone number, and a shipping address. The more sophisticated the convenience a user requires from Alexa, the more information Alexa (and, by proxy, Amazon) demands to accomplish each of the requested tasks. For example, in order for Alexa to place a phone call, she needs to gain access to a user's contact list or address book, which might include personal information about friends, family members, and even business associates.[74] In order to use Alexa to schedule appointments, a user must not only provide information about what kinds of services are required, but also grant Alexa access to cloud-based calendars.[75] To employ Alexa to hail an Uber, a user must grant Alexa access to her

---

69 *See* Aaron Paul Calvin*, Can Amazon's Alexa Be Your Friend?*, DIGG (Mar. 30, 2017, 9:44 PM), http://digg.com/2017/amazon-alexa-is-not-your-friend [https://perma.cc/34EP-3C5H].

70 *See id*.

71 *See* LITTLE SHOP OF HORRORS (Warner Bros. 1986).

72 *See* Calvin, *supra* note 69 (explaining that the more one uses the device, the more Alexa adapts to speech patterns, vocabulary, and personal preferences).

73 *See* Schwab, *supra* note 7.

74 *See* Jake Smith, *Amazon Alexa Calling: How to Set It Up and Use It on Your Echo*, ZDNET (May 30, 2017, 1:42 PM), https://www.zdnet.com/article/amazon-alexa-calling-how-to-set-it-up-and-use-it/ [https://perma.cc/F2JD-4T3L].

75 *See* Hugh Langley, *How to Link and Use Your Calendar with Alexa*, AMBIENT (July 19, 2019), https://www.the-ambient.com/how-to/schedule-sync-calendar-alexa-640 [https://perma.cc/UCJ5-QBHX].

GPS location data, the information about her destination, as well as direct access to the user's Uber account, which may contain credit card information, contact information, and other personal (or personally identifiable) information.[76] With each interaction, Alexa and her neural network become increasingly privy to larger volumes of a user's personal information and more entrenched in that user's daily life. Behind the scenes, Amazon gains greater access to the perpetual collection, storage, and manipulation of the user's information.

Part of Alexa's appeal is that she can be further tailored to cater to her user's every whim through the acquisition of "skills"—downloadable third-party add-ons, similar to mobile phone apps, that increase her aptitude, intelligence and functionality.[77] As of January 2019, the Amazon marketplace boasted over seventy thousand skills that Alexa had the potential to "learn."[78] Alexa's modularity and upgradeability increase her attractiveness as a virtual assistant and help to maintain the allure of the integrated invisible concierge experience that Amazon desires for its customers.

Amazon aspires for Alexa to permeate every facet of daily life[79]—to be omnipresent and indispensable.[80] Based on recent

---

[76] *See* Britta O'Boyle, *What Is Alexa and What Can Amazon Echo Do?*, POCKET-LINT (Dec. 26, 2018), https://www.pocket-lint.com/smart-home/news/amazon/138846-what-is-alexa-how-does-it-work-and-what-can-amazons-alexa-do [https://perma.cc/EV2X-RYFP]; *Privacy Policy: Data Collections and Uses*, UBER, https://privacy.uber.com/policy/ [https://perma.cc/XQS6-HV9Q] (effective May 25, 2018) (describing how Uber and its affiliates collect and use personal information to provide services). For a detailed explanation of personally identifiable information, see Campbell-Dollaghan, *supra* note 10.

[77] *See* Eric Griffith & Rob Marvin, *The Best Amazon Alexa Skills*, PC MAGAZINE (June 12, 2018, 5:40 PM), https://www.pcmag.com/article/352136/the-best-amazon-alexa-skills [https://perma.cc/EE7K-T9GY].

[78] *See* Dieter Bohn, *Amazon Says 100 Million Alexa Devices Have Been Sold—What's Next?*, VERGE (Jan. 4, 2019, 4:00 PM), https://www.theverge.com/2019/1/4/18168565/amazon-alexa-devices-how-many-sold-number-100-million-dave-limp [https://perma.cc/VM3Y-Q3DC].

[79] *See* Heather Kelly, *Amazon Wants Alexa Everywhere*, CNN BUS. (Sept. 22, 2018, 10:14 AM), https://money.cnn.com/2018/09/22/technology/alexa-everywhere/index.html [https://perma.cc/28QK-5F3H].

[80] *See* Scott Davis, *How Amazon's Brand and Customer Experience Became Synonymous*, FORBES (July 14, 2016, 2:50 PM), https://www.forbes.com/sites/scottdavis/2016/07/14/how-amazons-brand-and-customer-experience-became-synonymous/ [https://perma.cc/W6CG-5CP5].

statistics, the company is well on its way to achieving that goal. Although usually reluctant to divulge actual market share or sales figures, Amazon's Senior Vice President of Devices and Services, Dave Limp, recently revealed that as of January 2019, the company had sold over one hundred million Alexa-equipped devices worldwide[81] and increased its annual domestic Prime subscriptions by ten million to reach over one hundred million U.S. subscribers.[82] In light of these figures, it is interesting to note that over 150 Alexa-equipped products currently exist on the market, but fewer than fifty of those products are actually manufactured by Amazon.[83] Those two seemingly disparate figures coexist with Amazon's blessing because the true value to Amazon lies in the information that can be mined from users' adoption and integration of the AI, not in the nominal profit derived from the sale of the devices themselves.[84] Alexa extracts the data; therefore, Alexa exerts the power.[85]

C. The Rise and Influence of Big Data

Data collection and data mining—the siphoning and analyzing of a subject's data in order to predict future events or behaviors[86]—is not a novel concept borne out of the twenty-first century. On the contrary, its origins date back to at least the eighteenth century and

---

81 *See* Bohn, *supra* note 78. This figure represents total units sold containing Alexa; it does not break down by specific devices. *See id.*

82 *See* J. Clement, *Number of Amazon Prime Members in the United States as of June 2019*, STATISTA, https://www.statista.com/statistics/546894/number-of-amazon-prime-paying-members/ [https://perma.cc/84J6-LCN3] (citing that as of June 2019, Amazon had an estimated 105 million U.S. Amazon Prime subscribers).

83 *See id.*; *see also* Bohn, *supra* note 78.

84 *See* Tom Simonite, *Alexa Gives Amazon a Powerful Data Advantage*, MIT TECH. REV. (Jan. 18, 2017), https://www.technologyreview.com/s/603380/alexa-gives-amazon-a-powerful-data-advantage/ [https://perma.cc/GS83-HCMT]; *see also* Kelly, *supra* note 79.

85 *See* Antonio Garcia Martinez, *No, Data Is Not the New Oil*, WIRED (Feb. 26, 2019, 7:00 AM), https://www.wired.com/story/no-data-is-not-the-new-oil [https://perma.cc/G6PG-SC32]; *see also* Kelly, *supra* note 79.

86 Technically, data mining refers to the "computational process of discovering patterns in large data sets involving methods at the intersection of artificial intelligence, machine learning, statistics, Predictive analytics, and database systems," while data collection refers to "the process of gathering and measuring information usually with software." *See Data Mining vs Data Collection*, IMPORT.IO (Apr. 19, 2014), https://www.import.io/post/data-mining-vs-data-collection/ [https://perma.cc/AL37-QWCW]. In this Note, data mining and data collection are used somewhat interchangeably as the concept of Big Data as employed by companies like Amazon incorporates both.

the publication of Reverend Thomas Bayes' *An Essay Towards Solving a Problem in the Doctrine of Chances*, in which he outlined a formula that could analyze presented evidence to determine the statistical probability of an event's occurrence.[87] Drawing on the principles of conditional probability—the relation of current probability to prior probability—Bayes' Theorem described in mathematical terms how the likelihood of achieving one's desired hypothesis will be affected by the presentation of certain evidence or the knowledge of other probabilities.[88] Modern data scientists used Bayes' predictive theorem to form the foundational basis for all modern machine learning data mining.[89]

Although Bayes' Theorem had been used by mathematicians for over 250 years, it was not until the 1990s that significant advances in computer hardware, algorithms, and database technology finally allowed data scientists employed by retail and financial industries to analyze consumer data and recognize trends that would predict fluctuations in interest rates, stock prices, and customer demand, thus producing increases in their respective customer bases.[90] Built upon the data collection processes of the 1960s and the data access models of the 1980s, the 1990s version of data mining remained entrenched in a *retrospective* evaluation of the provided data.[91] In other words, the algorithms could identify trends and patterns in the data, but only as a result of what had occurred in the *past*. Big Data, the twenty-first century embodiment of data mining, however, is

---

87 *See* Thomas Bayes, *An Essay Towards Solving a Problem in the Doctrine of Chances*, *in* 53 PHIL. TRANSACTIONS 370, 414 (1763).

88 *See* Andrew Ellinor et al., *Bayes' Theorem and Conditional Probability*, BRILLIANT, https://brilliant.org/wiki/bayes-theorem/ [https://perma.cc/HX9Y-FLPD]; *see also* Rod Pierce, *Bayes' Theorem*, MATH IS FUN, https://www.mathsisfun.com/data/bayes-theorem.html [https://perma.cc/R5LN-ZH6J].

89 *See* Khyati Mahendru, *An Introduction to the Powerful Bayes' Theorem for Data Science Professionals*, ANALYTICS VIDHYA (June 13, 2019), https://www.analyticsvidhya.com/blog/2019/06/introduction-powerful-bayes-theorem-data-science/ [https://perma.cc/99GR-9WC6].

90 *See* Ray Li, *History of Data Mining*, HACKER BITS, https://hackerbits.com/data/history-of-data-mining/ [https://perma.cc/9YC2-HURV].

91 *See The History of Data Mining: Big Data*, EXASTAX BLOG (Jan. 20, 2017), https://www.exastax.com/big-data/the-history-of-data-mining/ [https://perma.cc/T5EJ-9U2S].

prospective.[92] It combines artificial intelligence and machine learning with data science and database theory to deliver comprehensive *predictive* analytics.[93] Put another way, today's data mining capabilities allow companies like Amazon to collect information that a consumer shares in the *present* and analyze the information in order to anticipate how that same consumer will act *in the future*.[94]

For Amazon, the use of Big Data translates into big profits.[95] Although the specifics behind Amazon's algorithms and analytics remain opaque, safeguarded behind the black box of proprietary trade secret information, the general concept driving its data collection is well known.[96] "We see our customers as invited guests to a party, and we are the hosts. It's our job every day to make every important aspect of the customer experience a little bit better," asserts CEO Jeff Bezos.[97] Bezos's desire to make life "better" for his customers translates into ensuring that a customer's transaction of goods and services through Amazon's sites and products remains both seamless and effortless.[98] To accomplish this, Amazon collects and stores copious amounts of data about its customers.[99] It then takes the collected data, analyzes it through proprietary algorithms, and generates predictive suggestions for products and services that each user might be inclined to purchase.[100] By employing targeted

---

92 "Big data analytics is the use of advanced analytic techniques against very large, diverse data sets . . . . [B]ig data comes from sensors, devices, video/audio, networks, log files, transactional applications, web, and social media—much of it generated in real time and at a very large scale." *Big Data Analytics,* IBM, https://www.ibm.com/analytics/hadoop/big-data-analytics [https://perma.cc/M2FA-J7YH].

93 *See The History of Data Mining: Big Data*, *supra* note 91.

94 *See* Alexander Furnas, *Everything You Wanted to Know About Data Mining but Were Afraid to Ask*, ATLANTIC (Apr. 3, 2012), https://www.theatlantic.com/technology/archive/2012/04/everything-you-wanted-to-know-about-data-mining-but-were-afraid-to-ask/255388/ [https://perma.cc/VTS2-HXHY].

95 *See* Jon Markman, *Amazon Using AI, Big Data to Accelerate Profits*, FORBES (June 5, 2017, 9:39 AM), https://www.forbes.com/sites/jonmarkman/2017/06/05/amazon-using-ai-big-data-to-accelerate-profits/#285c503a6d55 [https://perma.cc/V6GT-2X7P].

96 *See* Furnas, *supra* note 94.

97 Robert Binns, *Amazon CRM Case Study*, EXPERT MKT., https://www.expertmarket.co.uk/crm-systems/amazon-crm-case-study [https://perma.cc/E65V-3K7W].

98 *See id.*

99 *See* Lou Carlozo, *How Online Retailers Collect & Use Consumer Data*, DEALNEWS (Dec. 23, 2013), https://www.dealnews.com/features/How-Online-Retailers-Collect-Use-Consumer-Data/938928.html [https://perma.cc/8RPZ-KKGS].

100 *See id.*

advertising, utilizing content-specific upsells, and offering incentives such as Prime's free shipping, Amazon creates the perfect conditions to encourage and facilitate the completion of that purchase.[101] It is by purposeful design that Amazon endeavors to keep its users within its own ecosystem.[102]

D. The Harm of the Digital Dossier

The behaviorally tailored, predictive concierge experience that Amazon promises through Alexa requires the extraction of vast amounts of information from its users. Each encounter or "Interaction"[103] with a user helps Alexa to learn more about her subject. Because Alexa is voice-activated rather than text-based, the data recorded from Interactions provides Amazon with more than just digital bytes of information—it offers a user's context and intent.[104] Additionally, the placement of Alexa inside a private environment such as a home affects the quality of information to which the smart assistance is privy. Home users, viewing Alexa as a friend or confidante, feel extremely comfortable willingly[105] disclosing personal, sensitive, and sometimes even confidential information in her presence.[106] However, Alexa is neither a friend nor a confidante, but rather a sophisticated learning center whose main goal is to siphon information from her users for Amazon's gain. None of the information recorded is kept in confidence.[107] All

---

101 *See* Minda Zetlin, *Here's How Amazon Gets You to Buy More Stuff*, INC. (June 29, 2017), https://www.inc.com/minda-zetlin/heres-how-amazon-gets-you-to-buy-more-stuff.html [https://perma.cc/3J34-2QWZ].

102 *See* Kelly, *supra* note 79.

103 *See Alexa Terms of Use*, AMAZON, https://amzn.to/2FEchq5 [https://perma.cc/RX9J-P3J7]. "Interactions" is an Amazon-coined term for communiqués between Alexa and her subject. *Id.*

104 *See* Sarah Vizard, *Amazon Reveals How It Thinks About Advertising*, MARKETING WK. (Sept. 15, 2017), https://www.marketingweek.com/2017/09/15/amazon-reveals-advertising/ [https://perma.cc/29BM-LP84].

105 *See Alexa Terms of Use*, *supra* note 103.

106 *See, e.g.*, Calvin, *supra* note 69 (citing various examples of users who treat Alexa as a friend or confidante).

107 *See* Kate O'Flaherty, *Amazon Staff Are Listening to Alexa Conversations*, FORBES (Apr. 12, 2019, 11:54 AM), https://www.forbes.com/sites/kateoflahertyuk/2019/04/12/amazon-staff-are-listening-to-alexa-conversations-heres-what-to-do/#3a571b3671a2 [https://perma.cc/QY6H-6CX4] (explaining that Amazon's workers listen to the recordings and that experts have expressed that smart speakers are unsecured).

of the information gets transported over the internet back to Amazon's servers to be stored, manipulated, and re-purposed as Amazon sees fit.[108]

To be fair, the raw data that Amazon collects via Alexa has little to no value on its own. Amazon only derives value from the data once it is analyzed and synthesized by Amazon's algorithms to extract and produce secondary data sets that Amazon can then employ to more accurately predict the actions of its consumers.[109] This generated, proprietary data—what Harvard economist Shoshana Zuboff terms "behavioral surplus"[110]—is stored in perpetuity[111] within personalized digital dossiers[112] on Amazon's servers.[113] The subsequent use (or abuse) of this behavioral surplus drives surveillance capitalism,[114] creating and fostering a co-dependent and often exploitative relationship between data subjects and data brokers.[115]

---

[108] *See* Jennifer Pattison Tuohy & Hugh Langley, *Smart Home Privacy: What Amazon, Google and Apple Do with Your Data*, AMBIENT (Aug. 5, 2019), https://www.the-ambient.com/features/how-amazon-google-apple-use-smart-speaker-data-338 [https://perma.cc/29WB-L8TK].

[109] *See Data Is Giving Rise to a New Economy*, ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy [https://perma.cc/L9MM-GLGF] (explaining that data centers extract value from raw digital information).

[110] *See* John Naughton, *Welcome to the Age of Surveillance Capitalism,* GUARDIAN (Jan. 20, 2019, 2:00 AM), https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook [https://perma.cc/Z5NC-G9CU].

[111] *See Alexa, Echo Devices, and Your Privacy*, AMAZON, https://amzn.to/2YkU3kE [https://perma.cc/D6NN-NBEF]. *But see* Allison, *supra* note 68 and accompanying text.

[112] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY & PRIVACY IN THE INFORMATION AGE 1 (2004) (the term "digital dossier" is borrowed from this text).

[113] *See Where Does Amazon's Alexa Pull Data From?*, PROTECT AM.: HOME SECURITY BLOG (Dec. 23, 2017), https://www.protectamerica.com/home-security-blog/tech-tips/where-does-amazon-s-alexa-pull-data-from_15724 [https://perma.cc/E8RJ-KYGU].

[114] Surveillance capitalism refers to "selling access to the real-time flow of your daily life—your reality—in order to directly influence and modify your behavior for profit." Shoshana Zuboff, *The Secrets of Surveillance Capitalism*, FRANKFURTER ALLGEMEINE (May 3, 2016, 1:23 PM), https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html [https://perma.cc/Z5N9-VYJJ]. For a more in-depth explanation and exploration of the phenomenon and its impact on privacy today, see generally SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[115] *See* Naughton, *supra* note 110.

To be clear, the fact that Amazon collects information on its consumers—especially information provided with informed consent[116]—is not in and of itself harmful.[117] Further, Amazon's subsequent synthesis and analysis of the collected data does not suggest that the company has an inherent malicious or injurious intent toward its consumers. However, Amazon's massive aggregation and perpetual storage of its users' personal data, which is segmented into individualized digital dossiers and algorithmically employed to anticipate or influence the behavioral patterns of customers—all of which occurs in the absence of regulation—raises extreme concerns over the integrity and security of individuals' data privacy.

Data companies such as Amazon lure customers with the promise of convenience in exchange for an illusion of trust.[118] They ask that individual consumers trust them to allow for the installation of surveillance equipment and software into their most intimate spheres, such as the home. They ask that individuals trust them to effectively secure collected data, maintain its integrity, and employ the proceeds in the best interest of the consumer only. At no point do these companies substantively or legally define the parameters (or, quite frankly, even the meaning) of this implied trust, and rarely, if ever, do these companies reciprocate it.[119] Instead, companies hide

---

116 *See Alexa Terms of Use*, *supra* note 103.

117 *See, e.g.*, Mark Sullivan, *Actually, I Want to Hand Over Even More of My Personal Data to Big Tech*, FAST COMPANY (Mar. 19, 2019), https://www.fastcompany.com/90315789/actually-i-want-to-hand-over-even-more-of-my-data-to-big-tech [https://perma.cc/KE86-7Y7L] (arguing that there are benefits that can be derived from providing Big Tech personal data—i.e., "proactively remov[ing] the mundanities and friction points of everyday life, and know[ing] what I need practically before I do").

118 *See Alexa, Echo Devices, and Your Privacy*, *supra* note 111 ("Amazon knows that you care how information about you is used, and we appreciate your *trust* that we will do so carefully and sensibly."). (emphasis added).

119 *See, e.g.*, Warwick Ashford, *Uber Recognises Need for Consumer Trust After Breach Cover Up*, COMPUTERWEEKLY (Nov. 22, 2017, 10:30 AM), https://www.computerweekly.com/news/450430525/Uber-recognises-need-for-consumer-trust-after-breach-cover-up [https://perma.cc/7DD9-3FXT] (detailing how Uber covered up a customer data breach); Carly Page, *Amazon Suffers Data Breach but Remains Tight-Lipped on Details*, INQUIRER (Nov. 21, 2018), https://www.theinquirer.net/inquirer/news/3066757/amazon-data-breach-2018-black-friday [https://perma.cc/8DJ9-J2X3] (suggesting that there was more to the data breach than Amazon disclosed to its customers); Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

behind the impenetrable black box of algorithms and trade secrets to prevent individuals from knowing or understanding how their data is being processed, stored, and used (or reused).[120]

Absent comprehensive federal data privacy legislation to uniformly regulate the collection, storage, and manipulation of customer data, the only glue holding the current U.S. paradigm together is the illusive idea of trust that exists between the data consumer and the data collector. Professor Jack Balkin has embraced this notion of trust to advocate for a new regulatory model in which data collectors function as "information fiduciaries" on behalf of their consumers.[121] Drawing upon the tenets of agency law, Balkin argues that in the Digital Information Age where consumers have entrusted technology companies with their private data, those companies should be held to the same legal obligations as doctors or lawyers to act as fiduciaries and uphold the duties of care, confidentiality, and loyalty to use collected information in the best interest of the consumer only.[122] In this way, the illusion of trust that has been falsely established may continue unabated, but the consumer can rest easy knowing her data will be protected.

Mere trust alone, however, cannot shoulder the incredible burden of ensuring that data brokers such as Amazon will not abuse or breach the implied duties of confidentiality and loyalty owed to and expected by their users; mere trust alone cannot provide a remedy to

---

[https://perma.cc/N8UL-CEE6] (explaining how Facebook employed user data without consent).

120 *See* Tim Wu, *An American Alternative to Europe's Privacy Law*, N.Y. TIMES (May 30, 2018), https://www.nytimes.com/2018/05/30/opinion/europe-america-privacy-gdpr.html [https://perma.cc/UF7T-6N43] (explaining how companies like Amazon hold themselves as trustworthy yet fail to be transparent with their consumers about their data practices).

121 *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016); *see also* Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [https://perma.cc/6A47-JKCD].

122 *See* Balkin, *supra* note 121, at 1201, 1226.

an individual when one's data is breached,[123] misappropriated,[124] or employed in a manner that inflicts harm.[125] Further, as Lina Kahn and David Pozen recently articulated in their pushback to Balkin's information fiduciary theory, a user's trust in data collectors to handle their information with loyalty, confidentiality or care is wholly misplaced.[126] The end game of tech companies is profit; information equals profit, and current corporate law forbids putting the user's privacy needs ahead of the shareholder's bottom line.[127] As such, Big Tech companies such as Amazon will continue to push the boundaries of acceptable privacy norms, and it is only a matter of time before those boundaries will cease to be an effective bulwark from harm. As the tentacles of Big Data and Big Tech continue to embed themselves within the innermost sanctums of users' lives, it is imperative that the United States establishes an efficient legal framework to effectively regulate data collectors and to protect the personal data privacy interests of the consumer.

II. THE CURRENT U.S. PRIVACY FRAMEWORK: A SECTORAL REGIME RELIANT ON FIPPS, NOTICE AND CHOICE, AND THE FTC

A. A Difference in Approach: Comprehensive vs. Sectoral

When it comes to protecting the data privacy interests of the individual, the United States has long trailed behind its European

---

123 *See* Glenn Fleishman, *Equifax Data Breach, One Year Later*, FORTUNE (Sept. 7, 2018), http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/ [https://perma.cc/LU8P-SJWQ]; *see also* Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017, 1:27 PM), https://www.wired.com/story/equifax-breach-no-excuse/ [https://perma.cc/9LYJ-UZFF].

124 *See* Robinson Meyer, *The Cambridge Analytica Scandal, in Three Paragraphs*, ATLANTIC (Mar. 20, 2018), https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/ [https://perma.cc/ZNU3-C5E3].

125 *See* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#3b57679b6668 [https://perma.cc/5ZEB-FKFS] (explaining how Target used consumer data to determine a woman was pregnant before she had informed her family).

126 *See* Lina M. Kahn & David E. Pozen, *A Skeptical View of Information Fiduciaries*, HARV. L. REV. (forthcoming 2019) (manuscript at 1) (on file with author).

127 *See id*. at 6–10.

counterparts.[128] In large part, this is a result of intrinsic differences in the philosophies underlying the conceptions of personal and data privacy and the ways in which government should endeavor to oversee and regulate its protection. Having borne witness to the extermination of entire populations based on the whims of tyrannical regimes,[129] many countries within the EU vehemently protect individual privacy as a fundamental human right.[130] This freedom has since been codified in the EU Charter, which recognizes a right to privacy in one's personal data[131] as well as a "right to the respect of privacy" within one's home.[132]

In contrast, the United States, a country founded on the celebration of the individual and freedom of expression,[133] conceives of data as a personal and commercial asset[134] and privacy as a personal, autonomous choice.[135] Although the courts have inferred a general right to privacy in various amendments,[136] nowhere in the text of the

---

128 *See* Thomas Holt, *Data Privacy Rules in the EU May Leave the U.S. Behind*, GOV'T. TECH. (Jan. 24, 2019), http://www.govtech.com/computing/Data-Privacy-Rules-in-the-EU-May-Leave-the-US-Behind.html [https://perma.cc/HXM8-DV3C].

129 *See* Olivia B. Waxman, *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History*, TIME (May 24, 2018), https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/ [https://perma.cc/54F3-5NXZ] (positing that Nazi Germany and the Stasi's misuse of compiled personal data for heinous crimes has led to Europe's protective stance on privacy).

130 *See* Mark Scott & Natasha Singer, *How Europe Protects Your Online Data Differently Than the U.S.*, N.Y. TIMES (Jan. 31, 2016), https://www.nytimes.com/interactive/2016/01/29/technology/data-privacy-policy-us-europe.html [https://perma.cc/L7Y3-PN94].

131 *See* Charter of Fundamental Rights of the European Union art. 8, Oct. 26, 2012, 2012 O.J. (C 326) 391, 397 [hereinafter Charter of Fundamental Rights].

132 *See id*. art. 7, at 397.

133 *See* Taft Stettinius & Hollister LLP, *GDPR: How Is It Different from U.S. Law & Why This Matters?*, LEXOLOGY BLOG (Sept. 14, 2017), https://www.lexology.com/library/detail.aspx?g=4b2843f7-f67a-4015-bca9-96bd2fe344c9 [https://perma.cc/F23W-TLYN].

134 *See* Andrada Coos, *EU v US: How Do Their Data Privacy Regulations Square Off?*, ENDPOINT PROTECTOR BLOG (Jan. 17, 2018), https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/ [https://perma.cc/YY9W-AFGJ].

135 *See* Warren & Brandeis, *supra* note 23, at 198 (arguing that the law "secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others").

136 *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484–486 (1965) (inferring from the Fourteenth Amendment a right of marital privacy which should be protected against state restrictions on contraception); Katz v. United States, 389 U.S. 347, 359 (1967) (establishing within the Fourth Amendment the concept of a subjective expectation of

Constitution is such freedom explicitly guaranteed or safeguarded. Instead, the choice to maintain personal privacy receives limited constitutional and statutory protection from governmental intrusion[137] and relegates violations by private entities to the law of tort, contract, and other civil causes of action.[138] As Joel R. Reidenberg, a privacy expert at Fordham University School of Law, has observed, "In Europe the first line of defense against private wrongdoing is the state. In the U.S. our instinct is more liberal: Let private actors sue each other."[139]

The philosophical distinctions in privacy between the United States and the EU may also be evidenced in the current regulatory frameworks governing each. In May 2018, the EU enacted the General Data Protection Regulation ("GDPR"), an omnibus privacy legislation that comprehensively applies one unified code to all twenty-eight member states.[140] The GDPR imbues the individual with the power to control and regulate the collection, storage, and manipulation of his own personal information.[141] Acting as a privacy "bill of rights," the GDPR provides an individual with the right to know what types of information a business collects on him, to access the collected information, to rectify errors in the collected information, to withdraw consent at any time for the collection of such information, to object to the processing (or automated processing) of personal data, to port data, and to have any collected data permanently erased.[142]

---

privacy); Moore v. City of East Cleveland, 431 U.S. 494, 499 (1977) (finding unconstitutional a housing ordinance that invaded the privacy of an extended family's living arrangement).

137 *See supra* Section I.A.

138 *See* Richards & Solove, *supra* note 39, at 1918 (explaining the failure of the privacy torts to protect against the intrusion of the media or adapt to new privacy problems such as the collection of private data by businesses).

139 Bob Sullivan, *'La Difference' Is Stark in EU, U.S. Privacy Laws*, NBC NEWS (Oct. 19, 2006), http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/ [https://perma.cc/E575-PM2T].

140 *See generally* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

141 *See id.*

142 *See id.* ch. 3, arts. 15–22, at 43–46.

More than a mere piece of legislation, however, the GDPR represents a marked shift in the ethos and privacy norms that emerged in the E.U. post-9/11.[143] With the increased state surveillance following the attacks, individuals were particularly wary of disclosing information without providing explicit consent.[144] One of the aims of the GDPR was to rebuild consumer trust in sharing information with private companies.[145] Another aim of the GDPR was to limit the predatory practices of businesses.[146] "Data should not be kept simply because storage is cheap. Data should not be processed simply because algorithms are refined. Safeguards should apply, and citizens should have rights," declared EU Vice President and Justice Commissioner, Viviane Reding, during a 2014 European Data Protection Day celebration.[147] The aspirational principles that Reding has espoused in her speeches—consent, data minimization, purpose limitation, and confidentiality—are the same guiding principles that underscore and permeate the various facets of the GDPR.[148]

Consent forms one of the guiding cornerstones upon which the GDPR was built.[149] Before an individual's data may be collected, stored, or used, the company requesting the data must receive affirmative consent—unambiguously and voluntarily given—from the individual to do so, and such consent may be revoked at any time.[150] Data minimization requires that data processors[151]

---

143 *See* Trevor Butterworth, *Europe's Tough New Digital Privacy Law Should Be a Model for US Policymakers*, VOX (May 23, 2018, 6:45 AM), https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge [https://perma.cc/3XAY-BCL5].

144 *See* Viviane Reding, Vice-President, Eur. Comm'n, EU Justice Comm'r, Speech: A Data Protection Compact for Europe, (Jan. 28, 2014), *available at* http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm [https://perma.cc/6GFS-2M4D].

145 *See* Viviane Reding, Vice-President, Eur. Comm'n, EU Just. Comm'r, Speech: The EU Data Protection Reform: Helping Businesses Thrive in The Digital Economy, (Jan. 19, 2014), *available at* http://europa.eu/rapid/press-release_SPEECH-14-37_en.htm [https://perma.cc/75XF-M4MZ].

146 *See id.*

147 Reding, *supra* note 145; *see also* Butterworth, *supra* note 144.

148 *See generally* GDPR, *supra* note 141, art. 5, at 35–36.

149 *See generally id.* art. 7, at 37.

150 *See id.* art. 7(3), at 37.

151 Under the GDPR, "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." A

employ only as much data as is directly relevant and necessary to successfully accomplish a given task.[152] Moreover, any data collected must be limited to a one-purpose use and may not be repurposed without the express consent of the individual.[153] Companies are further required to maintain the integrity and confidentiality of all collected data[154] and to limit the length of time for which any personal data is stored.[155]

The comprehensive nature of the GDPR's regulation ensures continuity and cohesiveness in its application and enforcement across all EU member states for individual data and privacy protection. In upgrading from the aspirational guidance of the Data Protection Directive[156] to the mandatory and binding regulation of the GDPR, the EU signaled its commitment not only to protect individual data privacy, but also to establish itself as the de facto international standard for data privacy protection.

Eschewing the one-size-fits-all approach adopted by the EU and the GDPR, the United States, in contrast, has historically favored a sector-specific (sectoral) approach to privacy regulation, in which governmental interference is minimal, and the various industrial marketplace stakeholders dictate and determine internal oversight and governance on an as-needed basis.[157] The United States' *laissez faire* attitude toward privacy has resulted in the adoption of ad hoc statutory regulations passed only when exigent circumstances demand.[158] For example, in response to consumer outrage over the

---

"controller" is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." *Id.* art. 4(7)–(8), at 33.

152 *See id.* art. 5(1)(c), at 35.

153 *See id.* art. 5(1)(b), at 35.

154 *See id.* art. 5(1)(f), at 36.

155 *See id.* art. 5(1)(e), at 36.

156 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 23.

157 *See* Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY: PRIVACY + SECURITY BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/ [https://perma.cc/3YDS-SY64].

158 *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 10 Stat. 1936 (1996) ("HIPAA"), which regulates how PII is maintained by the healthcare and insurance industries; Gramm–Leach–Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999), which governs the collection and disclosure of customers' personal

rampant lack of transparency by credit companies who provided consumer data used to determine credit eligibility, Congress passed the Fair Credit Reporting Act,[159] which regulates the collection of credit information and access to credit reports.[160] Similarly, after Supreme Court nominee Robert Bork's video tape rental history was disclosed to a reporter during the nomination proceedings, the Washington, D.C. elite galvanized to pressure Congress to rapidly pass the Video Privacy Protection Act,[161] which creates liability for the "wrongful disclosure of video tape rental or sale records.[162] This fractured approach to regulation creates inconsistencies and irregularities among the various sectors.[163] Unlike the EU, the United States does not uniformly regulate or protect individual data privacy. Instead, each policy is based on the *type* of data collected and the *entity* responsible for aggregating and maintaining that collected data.[164] This overlapping patchwork of legislation has created confusion and contradictions for the consumer who acts as a data supplier, as well as the various entities that act as information and data collectors.[165]

B. The FIPPs

In the early 1970s, the development and incorporation of computer systems into the workplace led to technological advances in the collection and retention of personal data. Concerned about the potential for abuse of these new methods, the Secretary's Advisory

---

financial information by financial institutions; Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered section of 18 U.S.C.), which addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party Internet service providers.

159 15 U.S.C. § 1681 (2018).

160 *See* FED. TRADE COMM'N., DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014).

161 18 U.S.C. § 2710 (2018).

162 *See* Stephen Advokat, *Publication of Bork's Video Rentals Raises Privacy Issues*, CHI. TRIB. (Nov. 20, 1987), https://www.chicagotribune.com/news/ct-xpm-1987-11-20-8703270590-story.html [https://perma.cc/2NPA-M957].

163 *See* Solove, *supra* note 158.

164 *See* Solove, *supra* note 158.

165 For a more detailed explanation of the confusion that the U.S. privacy statutory scheme creates, see Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/ES6K-5DAQ].

Committee on Automated Personal Data Systems, under the direction of the Department of Health, Education and Welfare ("HEW"), supervised a study on record-keeping practices in the computer age, focusing on both government and business (the "HEW Report").[166] The committee recognized the harmful impact that unwanted disclosure of identifiable information might have on individuals and the protection of their personal privacy.[167] The committee's findings instigated the passage of both the Privacy Act of 1974,[168] which regulated the use of personal information by U.S. governmental agencies, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), which established international guidelines to facilitate the free flow of information between countries while simultaneously protecting personal data.

Arguably, however, one of the most impactful and lasting elements of the HEW report was the development of the Fair Information Practice Principles ("FIPPs"). The committee outlined five major principles[169]—transparency, use limitation, access and correction, data quality, and security—that should constitute a "minimum set of rights" available to the individual.[170] Broadly, these principles delineated an aspirational paradigm to address global concerns about the protection of individual data privacy within the ever-evolving technological landscape that threatened to erode it. The FIPPs further empowered individuals to actively participate in the collection and retention of their personal data.[171] Unfortunately, as adopted and implemented by U.S. law and the Federal Trade Commission in the 1990s, the broad idealistic principles of FIPPs were reduced to two narrow legal tenets, which serve as the backbone for the self-regulatory regime that

---

166 *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, DHEW PUB. NO. (OS) 73-94, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS ix (1973) [hereinafter HEW REPORT].

167 *Id.*

168 Privacy Act of 1974, 5 U.S.C. § 552a (1974).

169 *See* HEW REPORT, *supra* note 167, at xx.

170 *See* HEW REPORT, *supra* note 167, at xxi.

171 *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 341, 341–345 (Jane K. Winn ed., 2006).

dominates and protects the titans of the private sector: (1) notice and (2) choice.[172]

C. Notice and Choice

"Notice" implies transparency. It suggests that prior to gathering personal info, a data collection entity must only identify what information is being collected, how the collected information will be used, and whether any third parties might also obtain access to the collected information.[173] Traditionally the principle of notice has manifested itself through a company's privacy policy.[174] "Choice" has become synonymous with consent. It affords a user the opportunity to "opt-in" if one agrees to a company's proposed privacy terms. The "choice" element mainly manifests itself as the "agree" button that appears alongside the Terms of Service notifications prior to the download of apps, the entrance to a website, or the installation of software.

Supporters of "notice and choice" applaud the regime for its preservation of individual autonomy—it puts individuals in charge of decisions regarding the use and dissemination of their personal data.[175] The regime encourages users to be the arbiters of what is good or bad *for them*, without imposing further restrictions on others or the marketplace as a whole.[176] Professor Ryan Calo argues that this type of informed consent "furnishes consumers with information they would not otherwise have so that they can protect themselves and police the market."[177] Critics of "notice and choice," however, fault the regime as illusory, inadequate, and ineffectual.[178] Rather than empower individual autonomy, notice and choice anesthetizes and overwhelms, renders rational decision-making

---

172 *See id.* at 355–56.

173 *See* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 44 (2015) [hereinafter Reidenberg et al., *Disagreeable Privacy Policies*].

174 *See* WALDMAN, *supra* note 9, at 82.

175 *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1049 (2012).

176 *See id.* at 1028.

177 *Id.* at 1044.

178 *See generally* Cate, *supra* note 172.

meaningless,[179] and ultimately fails to address the real underlying issues of privacy and harm that the system was originally designed to remedy.

For notice to be effective, individuals must be able to read and understand the stated policies of the entities seeking to collect personal data. However, in today's world, where the sectoral regime encourages a lack of uniformity across data collection platforms, and almost all information flows are controlled by third parties, the achievement of true notice seems overwhelming, if not impossible. Lorrie Faith Cranor, director of the Carnegie Mellon Usable Privacy and Security Laboratory, estimates that in order for individuals to actually read through all the terms and conditions that are presented to them by third parties each year, they would have to devote between 180 to 300 hours a year, which roughly translates to dedicating about forty minutes each day.[180] Amazon's terms and conditions alone would take approximately nine hours to digest.[181] Because of the sheer effort involved to accomplish the task, few, if any, consumers ever read the relevant privacy policies posted by collectors of personal data, thereby rendering ineffective the concept of notice.

Even if an individual were to read each presented policy, it is unlikely that he or she would be able to fully comprehend its contents, so as to make the giving of consent—or choice—a truly informed decision.[182] Although several states have passed

---

179 *See* WALDMAN, *supra* note 9, at 84.

180 *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S 543, 563 (2008).

181 *See* Editorial, *How Silicon Valley Puts the 'Con' in Consent*, N.Y. TIMES (Feb. 2, 2019), https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html [https://perma.cc/Y4WC-8Z7S].

182 *See Most People Just Click and Accept Privacy Policies Without Reading Them—You Might Be Surprised at What They Allow Companies to Do*, NBR (Feb. 7, 2019), http://nbr.com/2019/02/07/most-people-just-click-and-accept-privacy-policies-without-reading-them-you-might-be-surprised-at-what-they-allow-companies-to-do/ [https://perma.cc/HS66-FGXX] (quoting Brian Vecci, the field chief technology officer for Varonis, a cybersecurity company that focuses on securing data: "[Privacy policies are] not designed for consumers, for you and me, to understand. They're written by lawyers for lawyers to protect the company"); *see also* Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR.: FACTTANK (Dec. 4, 2014), https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ [https://perma.cc/959Q-SZ6D] (quoting Joseph Turow, Professor of

legislation to require that companies write their online privacy policies in clear, precise, and non-legal language in order to help consumers better understand the scope of the information collected, such standardization has not been uniformly adopted nor federally mandated.[183] As a result, most companies pay lip service to satisfy the principle of "notice" by writing their policies in dense legalese,[184] with vague and ambiguous[185] language that obfuscates the true nature of the information being amassed and often forces individuals to consent to the collection of more data than necessary to accomplish a required task.[186] Thus, a vicious cycle ensues: company failures to adequately notify lead to consumer failures to properly choose.

Choice in today's oversaturated online market is not only illusory but often impossible. Choice should represent "giving consumers options as to how any personal information collected from them may be used."[187] However, because privacy policies are one-size-fits-all, and in practice cannot be tailored, altered, or user-customized, the once-empowering concept of autonomous choice has been essentially reduced to "choosing" between de facto acceptance of the stated terms or complete forfeiture of the use of the desired app, website, or software.

Communications and scholar of digital marketing and privacy issues at the University of Pennsylvania's Annenberg School for Communication: "Many people don't actually read privacy policies; they simply look at the label. . . . And the intuitive understanding—the cultural understanding—of the label is that when something says 'privacy policy,' it protects your privacy").

183 *See, e.g.*, California Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575–22579 (2004); CONN. GEN. STAT. § 42–471 (2017) (limited to businesses who collect Social Security numbers); DEL. CODE ANN. tit. 6, § 1205C (2015); NEV. REV. STAT. ANN. § 603A.340 (2017).

184 *See* Alan Henry, *Useable Privacy Shows You What Privacy Policies Actually Mean, in Plain English*, LIFEHACKER (Mar. 20, 2016, 2:00 PM), https://lifehacker.com/usable-privacy-shows-you-what-privacy-policies-actually-1764431489 [https://perma.cc/J8XB-M25Y]; *see also* Joseph Turow & Chris Jay Hoofnagle, *The FTC and Consumer Privacy in the Coming Decade,* 3 I/S 723, 731 (2006).

185 *See* Joel R. Reidenberg et al., *Ambiguity in Privacy Polices and the Impact of Regulation*, 45 J. LEGAL STUD. S163, S163–64 (2016).

186 *See* Reidenberg et al., *Disagreeable Privacy Policies*, *supra* note 174, at 46.

187 FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 8 (1998) [hereinafter FTC 1998 REPORT].

D. The FTC: The De Facto Privacy Regulator

Despite the publication of the HEW Report, the passage of the Privacy Act of 1974, and the decades-long warnings by consumer advocate groups of the potential for abuse of computerized record keeping, Congress has never created or even officially delegated oversight of consumer data privacy to any federal agency. Following a congressional invitation to investigate privacy risks posed by computer databases in the late 1990s, however, the FTC essentially volunteered to assume the watchdog mantle, and, over the past two decades, has steadily emerged as the country's de facto consumer privacy regulator.[188]

The FTC's effectiveness in regulating consumer privacy, however, has been hotly debated. Champions of the agency's efficacy hail its regulatory influence as "formidable."[189] Critics rebuke it as "toothless."[190] The reality lies somewhere in between. While the agency has made great strides in establishing an oversight regime where none previously existed, limits to its (1) chosen scope of enforcement, (2) statutory powers, and (3) physical capacity have ultimately diminished the FTC's ability to efficiently address and effectively curtail the onslaught of privacy concerns emerging from today's rapidly expanding and innovative tech sector.

The FTC derives its consumer regulatory authority from Section 5 of the Federal Trade Commission Act (the "Act" or "FTC Act").[191] Under the Act, the FTC has the power to investigate and resolve "unfair or deceptive acts or practices in or affecting commerce,"[192] with prosecution possible through both administrative and judicial proceedings.[193] Like most federal agencies, the FTC technically has

---

[188] For an in-depth look at how the FTC emerged as the privacy regulator, see generally Steven Hetcher, *The De Facto Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109 (2000).

[189] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COL. L. REV. 583, 600 (2014).

[190] *See* Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (June 28, 2012, 6:30 AM), https://www.wired.com/2012/06/ftc-fail/ [https://perma.cc/GU8W-LSFV].

[191] *See* 15 U.S.C. § 45 (2018).

[192] *Id.* § 45(a)(1).

[193] *See* FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE & LAW ENFORCEMENT AUTHORITY pt. 2, sec. A. (July 2008).

the ability to conduct oversight through adjudication[194] and rule-making.[195] However, the passage of the Magnuson–Moss Act[196] and the FTC Improvements Act of 1980[197] significantly curtailed the agency's ability to conduct oversight through rulemaking.[198] As a result, the agency has declined to promulgate comprehensive privacy-specific trade regulations, opting instead to monitor the private sector almost entirely through ad hoc adjudications.[199] While this case-specific process allows for flexibility and adaptability amid a rapidly expanding technological sector,[200] it ultimately limits the reach and sector-wide effectiveness of the FTC's oversight. Ad hoc adjudication commences only *after* a violation has occurred, whereas rulemaking can act prophylactically by proscribing violative behavior *before* it transpires.

The FTC is further limited by its statutory inability to proactively levy fines on businesses. Per Section 5 of the FTC Act, the FTC may only impose monetary sanctions on a business for violating an FTC cease and desist order or an FTC consent decree.[201] Substantially, this means that *before* a business will suffer any financial consequences for its violative actions, it must first commit an offense, be sanctioned by the FTC, agree to settle for that offense, and then commit that same offense *again* in violation of the original settlement agreement. This bureaucratic inefficiency allows for multiple transgressions to occur before a company has to proverbially "pay the piper." Similar to the issue with adjudications, the FTC's lack of authority to issue civil penalties against a

---

194 *See* 15 U.S.C. § 45(b) (2018).

195 *See id.* § 57(a).

196 15 U.S.C. §§ 2301–2312 (2018).

197 Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-52, §§ 7–12, 94 Stat. 374, 376–80.

198 *See* Barry B. Boyer, Executive Summary of *Barry B. Boyer Report: Trade Regulation Rulemaking Procedures of the Federal Trade Commission*, *in* 1979 ACUS RECOMMENDATIONS AND REPORTS 79–1, at 41.

199 *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 11 (2019) [hereinafter GAO-19-52]; *see also* Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1989 (2015).

200 *See* GAO-19-52, *supra* note 200, at 25.

201 *See* 15 U.S.C. § 45(m) (2018).

company for its *initial* violation reduces the agency's effectiveness in deterring harmful actions.

Section 5 of the FTC Act grants the agency expansive authority to protect consumers from deceptive practices or unfair methods of competition within the marketplace;[202] however, the FTC has elected to apply this broad mandate quite narrowly. To combat privacy concerns raised by the collection of consumer data in the emerging online landscape, the agency has chosen to focus on a market-based approach—encouraging "effective self-regulation" among private sector businesses rather than promulgating and instituting comprehensive sector-wide rules.[203] In a series of congressional reports issued in the late 1990s, the FTC advocated for businesses to employ the "core" FIPPs when designing consumers' informational privacy protections,[204] and further maintained that these principles should form the basis of any federal legislation or regulation involving the control of businesses' online consumer data collection.[205] In reality, however, the FTC eschewed many of the FIPPs and instead focused its oversight almost exclusively on notice (via "privacy policies") and choice (via "opt-in" mechanisms).[206] On the one hand, the agency's actions helped to foster the innovation, growth, and expansion of a nascent

---

202 *See id.* § 45(a), (n).

203 FTC 1998 REPORT, *supra* note 188, at 2.

204 In 1998 and 1999, the FTC advocated for five principles: (1) Notice/Awareness, (2) Choice/Consent, (3) Access/Participation, (4) Integrity/Security, and (5) Enforcement/Redress. *See id.*; *see also* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 3 (1999) [hereinafter FTC 1999 REPORT]. By 2000, however, the FTC had removed Enforcement/Redress as a core principle. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS iii (2000) [hereinafter FTC 2000 REPORT].

205 *See* FTC 1998 REPORT, *supra* note 188, at 7; FTC 1999 REPORT, *supra* note 205, at 3; FTC 2000 REPORT, *supra* note 205, at iii.

206 According to the FTC, "[n]otice" was the "most fundamental" principle, without which the other principles had no real meaning. *See* FTC 1998 REPORT, *supra* note 188, at 7; FTC 1999 REPORT, *supra* note 205, at 3. Although the reports discussed the principles of Access and Security, they left most of their recommendations on that front to the discretion of the businesses. "[T]he Commission believes that Access presents unique implementation issues that require consideration before its parameters can be defined." FTC 2000 REPORT, *supra* note 205, at 17. "The Commission believes that Security, like Access, presents unique implementation issues and that the security provided by a Web site should be 'adequate' in light of the costs and benefits." FTC 2000 REPORT, *supra* note 205, at 18.

online commercial industry;[207] on the other, the FTC's policies had the adverse effect of sanctioning predatory data collection methods by those same entities and industries.[208]

Further limiting the scope of its regulations, the FTC opts to bring most of its enforcement actions under the deceptive rather than unfair practices prong of Section 5 because the former is much easier to identify and police.[209] For the FTC to pursue a practice as "unfair," it must cause or be likely to cause "substantial injury to consumers," and must be one that consumers cannot reasonably avoid by other means.[210] Further, if a practice is "outweighed by countervailing benefits to consumers or to competition," the FTC will not deem it unfair.[211] Such a caveat establishes a particularly high threshold that is difficult to overcome when considering the predatory data collection practices that drive the surveillance economy. The FTC would prefer to focus on ad hoc adjudication of contract law disputes rather than perform the more difficult task of proactively promulgating data protection laws.

The FTC's almost singular focus on violations of notice and choice permits tech companies like Amazon to use their published privacy policies as shields against enforcement actions. Tech companies give notice and inform consumers of their data collection practices, however egregious they may be. In turn, customers rely on those same polices to become educated on the substantive level, if any, of protection that will be afforded to their personal data.[212] As these policies are readily available in written format, in the event that consumer data privacy has been breached, the FTC simply looks to see if any discrepancies exist between a data collector's proffered

---

207 *See* GAO-19-52, supra note 200, at 1.

208 *See* Turow & Hoofnagle, *supra* note 185, at 728 (arguing that the omission of the principles of "data minimization" and "purpose specification" from the FTC's recommendations has "led firms to collect extraneous information and repurpose information without consumer consent").

209 *See* David Lazarus, *FTC Is Falling Short in Protecting Consumers' Data Used by Businesses*, L.A. TIMES (Jan. 12, 2016, 3:00 AM), https://www.latimes.com/business/la-fi-lazarus-20160112-column.html [https://perma.cc/T9PM-9T3N].

210 15 U.S.C. § 45(n) (2018).

211 *Id.*

212 *See* Turow & Hoofnagle, *supra* note 185, at 744.

guidelines and the actions that it has taken.[213] Where a company has promised to provide protections yet failed to deliver (or delivered a lesser degree of) protection and privacy was breached (i.e., "broken promises"),[214] the FTC will endeavor to intervene.[215] Such intervention begins with an inquiry or warning, but more often than not, ends in a private settlement or consent decree. Over the past decade, the FTC has brought 101 privacy enforcement actions against companies, nearly all of which ended in consent decrees.[216] In many cases, the penalties inflicted by these consent decrees are so minimal that offending companies simply view them as a cost of doing business.[217] While such settlements may have an effect on an errant company's future behavior, they often fail to provide any remedy to the aggrieved consumer or even act as a deterrent to other companies.[218]

---

213 *See* WALDMAN, *supra* note 9, at 82; *see also* Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/73GH-52YN] (explaining that the fine was a result of "deceptive disclosures and settings" that undermined user privacy preferences).

214 *See* Solove & Hartzog, *supra* note 190, at 629.

215 *See, e.g.*, Eli Lilly & Co., 133 F.T.C. 763 (2002) (failure to protect confidentiality of user data); Microsoft Corp., 134 F.T.C. 709 (2002) (failure to limit collection of data to the purposes outlined in privacy policy); Genica Corp., FTC File No. 082 3113, Docket No. C-4252 (F.T.C. Mar. 16, 2009) (failure to provide adequate security for storage of personal data).

216 *See* GAO-19-52, *supra* note 200, at 22. The statistic refers to FTC internet privacy enforcement actions filed between July 1, 2008 and June 30, 2018 in which the agency alleged violations of either the FTC Act or the Children's Online Privacy Protection Act ("COPPA"). *See id.* at 21, 44. *But see* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015) (The FTC brought a claim against Wyndham alleging the company committed unfair practices and that its privacy policy was deceptive.); LabMD, Inc. v. Fed. Trade Comm'n, 776 F.3d 1275, 1277 (11th Cir. 2015) (LabMD brought a claim against the FTC challenging the agency's efficacy in bringing enforcements proceedings).

217 *See* Michelle de Mooy, *How to Strengthen the FTC Privacy & Security Consent Decrees*, CDT BLOG (Apr. 12, 2018), https://cdt.org/blog/how-to-strengthen-the-ftc-privacy-security-consent-decrees/ [https://perma.cc/R6J4-798K].

218 *See* GAO-19-52, *supra* note 200, at 21; *see also* Nitasha Tiku, *Why Facebook's 2011 Promises Haven't Protected Users*, WIRED (Apr. 11, 2018, 9:02 PM), https://www.wired.com/story/why-facebooks-2011-promises-havent-protected-users/ [https://perma.cc/RJ4A-Q7EH]; Sarah Frier, *Former FTC Technologist Says Facebook Violated Consent Decree,* BLOOMBERG (June 19, 2018, 4:56 PM), https://www.bloomberg.com/news/articles/2018-06-19/former-ftc-technologist-says-facebook-violated-consent-decree [https://perma.cc/L9UU-46N3].

Moreover, the FTC is hamstrung by personnel constraints, which further restrict its capacity to regulate and enforce. "Our tools are limited," admits Maneesha Mithal, Associate Director of the FTC's Division of Privacy and Identity Protection.[219] Despite reports that data privacy and the uncontrolled collection of consumer data remain some of the biggest threats facing the nation,[220] the FTC, as the de facto privacy agency, staffs only forty full-time privacy employees and five full-time technologists.[221] This pales in comparison to the 500-person staff of the United Kingdom Information Commissioner's Office or the 110-person staff of Ireland's Data Protection Commissioner.[222] The FTC literally fails to employ enough people at the agency to adequately monitor and enforce the increasing threats to privacy resulting from the rapid expansion of technology and data collection within the private tech sector.[223]

Since the FTC has taken up the mantle of federal privacy watchdog, it has achieved much good.[224] However, the limitations placed on the agency by its narrow scope of focus, statutory restrictions, and physical constraints have produced a quasi-regulatory regime ill-suited to adapt to a rapidly changing technological landscape that increasingly threatens consumer data privacy. Rather than create preemptive rules that anticipate privacy concerns *before* they erupt into problems, the FTC has instead opted for ad hoc individual

---

219 Lazarus, *supra* note 209.

220 *See, e.g.*, *Rethinking Privacy for the AI Era*, FORBES: INSIGHTS (Mar. 27, 2019, 1:16 PM), https://www.forbes.com/sites/insights-intelai/2019/03/27/rethinking-privacy-for-the-ai-era/ [https://perma.cc/EFX4-F475]; *see also* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 30, 33 (Jan. 2016).

221 *See* Cat Zakrzewski, *The Technology 202: The Government's Top Silicon Valley Watchdog Only Has Five Full-Time Technologists. Now It's Asking Congress for More.*, WASH. POST (Apr. 4, 2019, 8:47 AM), http://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/04/04/the-technology-202-the-government-s-top-silicon-valley-watchdog-only-has-five-full-time-technologists-now-it-s-asking-congress-for-more/5ca512661b326b0f7f38f30d/ [https://perma.cc/3BTV-3S2L].

222 *See id.*

223 *See, e.g.*, Maass, *supra* note 191 (citing multiple examples where FTC oversight was "scooped" by investigative journalists, foreign agencies, and even ambitious graduate students).

224 *See generally* Solove & Hartzog, *supra* note 190.

adjudications that are piecemeal and *reactive*.[225] Rather than broaden the scope of its enforcement to prosecute *unfair* practices, the FTC has chosen instead to primarily focus on the easier-to-monitor prong of *deceptive* practices. Consequently, the FTC—the agency best suited to aggressively and proactively enforce consumer data privacy safeguards in the new Digital Age of AI—allows Big Data and Big Tech to push the boundaries of the law, to ask for forgiveness rather than permission, and to continue to treat consumer data as their own personal asset.

III. THE LAW'S TREATMENT OF THE COLLECTION OF CONSUMER DATA BY AI

A. The Failure of Notice and Choice to Protect Consumers

In an ideal world, the data privacy laws of the United States would protect individuals from three categories of harms that could result from the unauthorized collection, unsafe storage or unlicensed use of their data: (1) harm to their reputation or autonomy (from the involuntary release or use of confidential information); (2) harm to their right of access (resulting from discrimination or bias in the misuse of information); and (3) harm to their financial and economic stability (resulting from a breach or theft of protected information).[226] Unfortunately, with its lack of comprehensive federal directives, its focus on sectoral oversight heavily reliant on the principles of "Notice and Choice," and its emphasis on industry self-regulation, the current data privacy paradigm in the United States provides no such consumer safeguards. The current privacy framework concentrates almost solely on providing consumers with information in order to create the illusion of control over their data and privacy, and, in doing so, ignores the more crucial element of providing protection for the consumer from predatory data collection practices. This framework puts too much onus on the individual

---

[225] For a counter argument that suggests that FTC jurisprudence has developed a comprehensive body of "law" akin to the common law, see generally Solove & Hartzog, *supra* note 190.

[226] *See* Alan McQuinn, *Understanding Data Privacy*, REAL CLEAR POL'Y (Oct. 25, 2018), https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html [https://perma.cc/6EFY-2X7Y].

to make "informed" choices and not enough responsibility on the companies to refrain from engaging in abusive activity or the federal government to police such violations. The current U.S. data privacy regime assumes too much and delivers too little.[227]

Moreover, the law treats the tech sector's data collection practices as one-size-fits-all, with almost no distinction made across divergent platforms about how information is collected, stored or used. For example, under current U.S. law, Amazon's AI-facilitated collection of user data via Alexa receives the same legal treatment as Amazon's manual collection of user data through its website or mobile app.[228] In both instances, the law simply expects that Amazon will choose on its own to implement a fair and trustworthy process of data collection by providing users with conspicuous "notice" of its privacy and collection policies and allowing them the "choice" to opt-out of the use of Amazon's services should they disagree.

For its part, Amazon complies fully with the law's prescriptions.[229] The company conspicuously posts its privacy policy explaining its data collection practices on its site,[230] and it allows users the choice of whether or not to avail themselves of the tools within the Amazon ecosystem.[231] Because the concept of engendering consumer trust is embedded in the company's cultural

---

227 *See supra* Section II.C.

228 *See, e.g.*, Dickinson Wright, *The Internet of Toys: Legal and Privacy Issues with Connected Toys*, LEXOLOGY (Dec. 5, 2017), https://www.lexology.com/library/detail.aspx?g=73ff6361-5a5e-4511-9a12-95da0e16bd63 [https://perma.cc/QX7Y-33PV] (acknowledging that "the law is behind the technology" and describing how the current sectoral laws and FTC guidelines apply similarly to data collection across various IoT gadgets). *But see* James Thorne, *Amazon Adds HIPAA Compliance to Alexa Skills, Opening Door for Secure Health Apps*, GEEKWIRE (Apr. 4, 2019, 7:31 AM), https://www.geekwire.com/2019/amazon-adds-hipaa-compliance-alexa-skills-opening-door-secure-health-apps/ [https://perma.cc/HU26-CKRZ] (explaining that Alexa's collection of PII via its new health skills is governed by HIPAA).

229 As of this writing, Amazon has a conspicuously posted privacy policy and has never been charged by the FTC with deceptive or unfair practices in relation to its privacy or data collection policies. *See infra* note 231.

230 *See Amazon Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010 [https://perma.cc/TQ53-CVKJ].

231 *Id.* ("You can choose not to provide certain information, but then you might not be able to take advantage of many of our features.").

ethos,[232] Amazon goes a step further in its policies' inclusions, providing examples of the types of information the company collects,[233] the ways in which it collects it,[234] how it shares that information with third parties,[235] and how individuals might access their collected data.[236] Provided that Amazon then abides by its posted policies, it has satisfied all of the elements necessary to comport with existing federal privacy standards.

But what about the protection of the consumer? Is Amazon's mere compliance with "Notice and Choice" enough to provide a comprehensive or transparent assessment of Amazon's intent for all of the data collected? Does Amazon's inclusion of a legal disclaimer that their privacy policy can and will be amended based solely on the company's whims[237] inherently negate any suggested protection implied by the policy itself, or make impossible customer reliance

---

232 *See* David Marino-Nachison, *Jeff Bezos: Customer Trust 'Is What Allows You to Expand'*, BARRON'S (Sept. 4, 2018, 5:04 PM), https://www.barrons.com/articles/jeff-bezos-customer-trust-is-what-allows-you-to-expand-1536095054 [https://perma.cc/S2KN-2ZT7] (quoting Jeff Bezos: "[Customer trust is] very valuable, and so you would never do anything to jeopardize it.").

233 *See Amazon Privacy Notice*, *supra* note 231.

234 *See id*.

235 *See id*.

236 *See id.* ("Amazon.com gives you access to a broad range of information about your account and your interactions with Amazon.com for the limited purpose of viewing and, in certain cases, updating that information."). The "broad access" that Amazon purports to give, however, is extremely limited to the raw data that the user initially provides, rather than the algorithmically generated data that Amazon subsequently employs. Amazon provides the following as examples of available data:

> Examples of information you can access easily at Amazon.com include up-to-date information regarding recent orders; personally identifiable information (including name, e-mail, password, communications and personalized advertising preferences, address book, and 1-Click settings); payment settings (including credit card information and promotional certificate and gift card balances); e-mail notification settings (including Product Availability Alerts, Delivers, and newsletters); Recommendations (including Recommended for You and Improve Your Recommendations); shopping lists and gift registries (including Wish Lists and Baby and Wedding Registries); Seller accounts; and Your Profile (including your product Reviews, Recommendations, Listmania lists, Reminders, personal profile, and Wish List).

Id.

237 *See id*.

upon it? The ambiguity and lack of complete transparency sanctioned by the current data privacy paradigm of "Notice and Choice" might insulate businesses from legal claims or FTC inquiry, but they leave consumers and their data vulnerable to misappropriation, mishandling, and misuse.

Amazon's products and services are uniformly governed by a blanket privacy policy.[238] When a user first creates an Amazon account to enter its ecosystem, she sees the following notification: "By creating an account, you agree to Amazon's Conditions of Use and Privacy Notice,"[239] written in small font beneath the required log-in fields. The qualification contains a link, which redirects the user to the referenced Conditions of Use and Privacy Notice. Once a user clicks "sign in," no further affirmative action is required to assent to Amazon's terms or policies. Such "acceptance by use" is known legally as a browse-wrap agreement and has become a standard method by which tech companies comply with "notice."[240] The mere act of creating an Amazon account or using an Alexa device makes consent to Amazon's policies less a "choice" and more a *fait accompli*.

The means by which a user interfaces with Alexa can further blur the lines of consent. Unlike manually typing items into a search bar or mouse clicking a button, an Alexa user simply queries aloud as though engaged in conversation with an actual person. Alexa's natural-language processing erases any tactile reminder that one's data is constantly being collected or stored. The convenience and ease of using the hardware masks the surreptitious and constant surveillance of its software. As a result, Alexa users may be lulled into a false sense of security to feel comfortable disclosing to Amazon more data than necessary to achieve a requested task—all with little understanding as to how this data fed to Alexa might be stored or used by Amazon in the future.[241]

---

238 *See Amazon Privacy Notice*, *supra* note 231.

239 *See Registration,* AMAZON, https://amzn.to/2X38E2K [https://perma.cc/6DEB-NJKX].

240 *See* Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up to Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173, 174 (2007) (defining "browse-wrap" as an agreement "typically presented at the bottom of the Web site where acceptance is based on 'use' of the site").

241 *See* WALDMAN, *supra* note 9, at 141–46.

While tech companies such as Amazon tout their adherence to the self-regulatory practice of "privacy by design,"[242] the loopholes deliberately embedded into online interfaces, legal disclaimers, and AI collection render ineffective the federal government's outdated regime of "Notice and Choice" as a means to protect users and their privacy from predatory data collection practices.[243] As Professor Woodrow Hartzog argues, "Every aspect of the user experience is designed to extract data out of [the user], to get [the user] to never stop sharing, and to have [the user] feel good about it in the process."[244]

When the FTC initially embraced "Notice and Choice" as the cornerstone for consumer data privacy protection, technology was limited,[245] data storage was prohibitively expensive,[246] and data collection through intermediaries was a mere by-product of the service offered rather than the service itself.[247] As a result, companies were more selective in the type of data they would collect and would maintain only as much information as was necessary for their

---

[242] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018).

[243] *See* Sacha Molitorisz, *It's Time for Third-Party Data Brokers to Emerge from the Shadows*, CONVERSATION (Apr. 4, 2018, 2:46 AM), https://theconversation.com/its-time-for-third-party-data-brokers-to-emerge-from-the-shadows-94298 [https://perma.cc/ULH9-WLJJ].

[244] Daniel Solove, *Should Privacy Law Regulate Technological Design? An Interview with Woodrow Hartzog*, TEACHPRIVACY (Apr. 12, 2018), https://teachprivacy.com/should-privacy-law-regulate-technological-design-an-interview-with-woodrow-hartzog/ [https://perma.cc/6J7C-Z592].

[245] *See* Cameron F. Kerry, *Proposed Language for Data Collection Standards in Privacy Legislation,* BROOKINGS (Apr. 16, 2019), https://www.brookings.edu/blog/techtank/2019/04/16/proposed-language-for-data-collection-standards-in-privacy-legislation/ [https://perma.cc/7BXV-BHQC].

[246] *See* Lucas Mearian, *CW@50: Data Storage Goes from $1M to 2 Cents per Gigabyte*, COMPUTERWORLD (Mar. 23, 2017, 3:00 AM), https://www.computerworld.com/article/3182207/cw50-data-storage-goes-from-1m-to-2-cents-per-gigabyte.html [https://perma.cc/7U6M-HV73] (explaining that in 1967 one gigabyte of hard drive storage would have cost one million dollars, while today it costs two cents); *see also* HEW REPORT, *supra* note 167, at 22.

[247] *See* Steven Melendez & Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST COMPANY (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information [https://perma.cc/4Y5G-4FQ3].

immediate purposes.[248] But times have changed.[249] Thanks in large part to Amazon,[250] cloud storage today is cheap and scalable, and the proliferation of voice-activated AI smart assistants has exponentially increased the scope of data collection.[251] The pairing of Alexa's voice-activated, always-on surveillance with Amazon's unlimited cloud server space allows for unrestricted harvesting, storage, and manipulation of user data, in which individuals are often unwittingly consenting to the perpetual and constant collection of their voice, their image, their likes, their habits, their questions, and, essentially, their thoughts.[252]

"Mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[253] The siphoning of one's inviolate personality—the *very* harm that Warren and Brandeis warned against over one hundred years ago—is *still* happening today.[254] In 1890 Warren and Brandeis were focused on addressing two new technological inventions: the portable recording device and the portable camera.[255] Today, these "mechanical devices" have proliferated and invaded all spheres of our personal space. They exist in our homes, our cars, our offices, and most ubiquitously, our pockets. Although the

---

248 *See* Kerry, *supra* note 246.

249 *See* Scott Fulton III, *Amazon AWS: Complete Business Guide to the World's Largest Provider of Cloud Services*, ZDNET (Apr. 1, 2019), https://www.zdnet.com/article/amazon-aws-everything-you-should-know-about-the-largest-cloud-provider/ [https://perma.cc/4M3E-PPU7].

250 *See id.* ("Today, Amazon is the world's largest provider of computing services accessible through the web from globally distributed servers in highly automated data centers."). In 2018, AWS grew forty-seven percent and accounted for the majority of the company's profits that fiscal year. *See* Stephanie Condon, *In 2018 AWS Delivered Most of Amazon's Operating Income*, ZDNET (Jan. 31, 2019), https://www.zdnet.com/article/in-2018-aws-delivered-most-of-amazons-operating-income/ [https://perma.cc/AD34-RU9T].

251 *See* Keith D. Foote, *A Brief History of Data Storage*, DATAVERSITY (Nov. 1, 2017), https://www.dataversity.net/brief-history-data-storage/ [https://perma.cc/EZK8-D9CS].

252 *See The Learning Machine: Amazon's Empire Rests on Its Low-Key Approach to AI*, ECONOMIST (Apr. 11, 2019), https://www.economist.com/business/2019/04/13/amazons-empire-rests-on-its-low-key-approach-to-ai [https://perma.cc/T7R3-WW2K] (explaining that Amazon is one of AWS' biggest customers); *see also* HARTZOG, *supra* note 243, at 248–49.

253 Warren & Brandeis, *supra* note 23, at 195.

254 *See id.* at 205, 211.

255 *See* WALDMAN, *supra* note 9, at 16.

technology of these "mechanical devices" has advanced exponentially, the injury to the individual—the intrusion into one's private space—remains the same. Unfortunately, 130 years later, the law has failed to evolve to adequately address these concerns.[256]

B. Amazon Home. Amazon Health. Amazon, Help!: A Cautionary Tale

A user's purchase of a voice-enabled Alexa smart assistant device signifies more than merely the acquisition of a high-end technical gadget; it represents the "filing [of] citizen papers for the digital duchy of Amazonia."[257] Amazon wants Alexa and its data-collecting AI to be ubiquitous; Amazon wants to siphon as much personal data from its users as possible.[258] Therefore, when a consumer opts to buy an Alexa, she makes more than a simple utilitarian decision based on product functionality; rather, she chooses to adopt an ecosystem into her life and her home—similar to adopting a pet—albeit a pet with a doctorate in statistical analysis and a highly sophisticated algorithm that can track and analyze every aspect of every interaction.[259]

Quantitative futurist Amy Webb, founder of the Future Today Institute, predicts that by 2029 most of the population will live in smart homes—domiciles designed for a 24/7 concierge experience, in which a singular AI (such as Amazon's AI, Alexa) controls, and the entire house runs on the algorithmic data outputs of its

---

[256] *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (Plaintiff alleged misinformation posted only by the defendant caused harm to his employment prospects, which in turn caused him increased anxiety and stress.). The Court dismissed the suit for lack of Article III standing for failure to plead a tangible or "concrete" injury—one that was "real, and not abstract." *Id*. at 1548. This ruling has severely limited the avenues for redress for many data subjects who have experienced only reputational or "intangible" harms as a result of the misuse of their data.

[257] Steven Levy, *Jeff Bezos Owns the Web in More Ways Than You Think,* WIRED (Nov. 13, 2011, 9:00 PM), https://www.wired.com/2011/11/ff_bezos/ [https://perma.cc/42AA-8AX9].

[258] *See* Steve Wasserman, *The Amazon Effect,* NATION (May 29, 2012), https://www.thenation.com/article/amazon-effect/ [https://perma.cc/R9WP-RPG2].

[259] *See* Ken C. Pohlmann, *Big Data and You: The Analytics of Amazon's Alexa*, SOUND & VISION (Apr. 11, 2017), https://www.soundandvision.com/content/analytics-alexa [https://perma.cc/9JL3-TUED] (explaining the technology behind Alexa).

inhabitants.[260] To many, this scenario sounds blissfully idyllic. After all, few would balk at the convenience and efficiency of a personalized assistant with the ability to analyze and anticipate every interaction in order to remain a step ahead of one's personal needs at all times. But Webb's vision paints a more cautionary tale.[261] A smart home, in which every gadget is Alexa-enabled, would provide literal 24/7 surveillance of its inhabitants, which translates to 24/7 collection of their data, steadily streamed to digital dossiers, stored in perpetuity on Amazon's cloud servers.[262] This around-the-clock perpetual surveillance would allow Amazon to peek behind the curtain and gain access to a more comprehensive representation of the consumer and her family.[263] Although singularly some of the raw data collected may appear harmless or even trivial, when synthesized in the aggregate, such seemingly innocuous data can lead to harmful and unintended consequences—especially when that data is coupled with other pieces of collected information, analyzed, and re-purposed to predict or affect future situations.[264]

Amazon may have begun as a simple online bookseller,[265] but it has grown into a multi-hyphenate conglomerate with tentacles in a

---

[260] *See* Schwab, *supra* note 7 (describing Amy Webb's vision for the future); *see also Welcome to Your Connected Home*, AMAZON, https://www.amazon.com/b?node =13295231011 [https://perma.cc/J3S8-LYBB]; Jared Newman, *With Cheap New Smart Home Gear, Amazon Wants to Keep You in Its World*, FAST COMPANY (Oct. 6, 2018), https://www.fastcompany.com/90241614/with-cheap-new-smart-home-gear-amazon-wants-to-keep-you-in-its-world [https://perma.cc/C33G-CG6X].

[261] *See id.*

[262] *See id*.

[263] *See id*.

[264] *See id.* (describing how Amazon may from ambient noise be able to detect who else is in the room and even discern from a voice whether one is sick or depressed); *see also* Louise Matsakis, *The Wired Guide to Your Personal Data (And Who Is Using It)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection/ [https://perma.cc/S6AK-JCC6] ("Even seemingly benign activities, like staying in and watching a movie, generate mountains of information, treasure to be scooped up later by businesses of all kinds.").

[265] *See* Avery Hartmans, *15 Fascinating Facts You Probably Didn't Know About Amazon*, BUS. INSIDER (June 17, 2019, 2:47 PM), https://www.businessinsider.com/jeff-bezos-amazon-history-facts-2017-4; *see also Amazon Studios*, AMAZON, https://studios. amazon.com/ [https://perma.cc/Q93Q-3BDC].

myriad of retail markets ranging from entertainment[266] to grocery[267] to cloud computing.[268] While on the surface Amazon's expansion into various marketplaces may look like mere portfolio diversification, a deeper analysis reveals that each extension of its realm provides the company increased opportunities to collect consumer data.[269] To date, much of Amazon's collected data has been employed to better predict, streamline, and facilitate users' transactions and purchases on its retail site.[270] However, it begs the question, what might happen to the copious amounts of user data that Amazon has already collected should the company branch out into other non-retail sectors, such as healthcare?

In January 2018, Amazon announced a joint partnership with JP Morgan Chase and Berkshire Hathaway, signaling its entrée into the data-driven healthcare sector.[271] In November 2018, Amazon launched Amazon Comprehend Medical, "a new HIPAA-eligible machine learning service that allows developers to process unstructured medical text and identify information such as patient diagnosis, treatments, dosages, symptoms and signs."[272] In April

---

266 *See* Saquib Shah, *Amazon Will Become a Bona Fide Film Studio This Year*, ENGADGET (July 31, 2017), https://www.engadget.com/2017/07/31/amazon-film-studio/ [https://perma.cc/S5BZ-KJRQ]; *see also Amazon Studios*, *supra* note 266.

267 *See* Nick Wingfield & Michael J. de la Merced, *Amazon to Buy Whole Foods for $13.4 Billion*, N.Y. TIMES (June 16, 2017), https://www.nytimes.com/2017/06/16/business/dealbook/amazon-whole-foods.html [https://perma.cc/E8AP-2E3L].

268 *See Cloud Computing with AWS*, AMAZON, https://aws.amazon.com/what-is-aws/ [https://perma.cc/Z93L-AJJK].

269 *See* Greg Petro, *Amazon's Acquisition of Whole Foods Is About Two Things: Data and Product*, FORBES (Aug. 2, 2017, 12:13 PM), https://www.forbes.com/sites/gregpetro/2017/08/02/amazons-acquisition-of-whole-foods-is-about-two-things-data-and-product/#3ada9d4ba808 [https://perma.cc/2EKS-Z5VB]; *see also* Mike Sands, *How Amazon Is Minting a New Generation of Customer-Data-Obsessed Companies*, FORBES (Mar. 2, 2018, 10:21 AM), https://www.forbes.com/sites/mikesands1/2018/03/02/how-amazon-is-minting-a-new-generation-of-customer-data-obsessed-companies/#19fa09d28ed7 [https://perma.cc/7T7K-EW42].

270 *See The Learning Machine*, *supra* note 252; *see also* Sands, *supra* note 269.

271 *See* Nick Wingfield et al., *Amazon, Berkshire Hathaway and JPMorgan Team Up to Try to Disrupt Health Care*, N.Y. TIMES (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/technology/amazon-berkshire-hathaway-jpmorgan-health-care.html [https://perma.cc/7KM4-LEC2].

272 Andis Robeznieks, *Amazon's Health Care Push Expands to Machine Learning for the EHR*, AMA (Nov. 28, 2018), https://www.ama-assn.org/practice-management/digital/amazon-s-health-care-push-expands-machine-learning-ehr [https://perma.cc/2JDT-U38K].

2019, Amazon announced the release of its first set of HIPAA-compliant Alexa skills.[273] Although "Prime Health" has yet to materialize, it remains only a matter of time before that occurs, according to investor John Doerr.[274] Once that happens, Amazon's vault of collected user data and its ability to effectively manipulate that data with its algorithms will give the company an edge in a sector that has been notoriously reluctant to embrace new technology.[275]

The kind of lifestyle and biometric data that Alexa's AI can now collect from its vantage within the home will have tremendous worth when it is (inevitably) applied in the context of healthcare, predicts Webb.[276] Consider the following hypothetical scenario: In an Alexa-enabled smart home, User X wakes every morning at 8:30 and tasks Alexa with calling an Uber to take him to work. User X comes home every evening around 6:30, plops himself on the couch, and watches five hours of peak television courtesy of Amazon Prime. At approximately 11:30 each night, User X yells from his couch for Alexa to order him a large pizza with all of the preferred toppings and a two-liter bottle of soda. User X is a creature of habit, so this routine repeats daily. Amazon collects *all* of this information—the wake-up time and, relatedly, how much time has been spent asleep, the destinations of the Uber rides, the types of television programs watched, the amount of pizza and soda consumed—all under the

---

[273] *See* Natalie Gagliordi, *Amazon Launches HIPAA-Compliant Alexa Skills for Healthcare*, ZDNET (Apr. 4, 2019, 9:00 PM), https://www.zdnet.com/article/amazon-launches-hipaa-compliant-alexa-skills-for-healthcare/ [https://perma.cc/5Q5W-225T].

[274] *See* Mark Sullivan, *Amazon Prime Health Is Coming, According to an Early Investor*, FAST COMPANY (Nov. 30, 2018), https://www.fastcompany.com/90274630/amazon-prime-health-is-coming-according-to-an-early-investor [https://perma.cc/S5B9-MAE6].

[275] *See id.*

[276] *See* Schwab, *supra* note 7; *see also* Molly Wood, *Amazon Is 25 Years Old. What Will the Company's Next Chapter Look Like?*, MARKETPLACE (July 2, 2019), https://www.marketplace.org/shows/marketplace-tech/amazon-is-25-years-old-what-will-companys-next-chapter-look-like/ [https://perma.cc/6NSB-BY3F] ("Once the boxes and the things that we've ordered arrived at our homes, the data pipeline gets shut off. If you're suddenly now talking to all the different devices in your home (speakers, microwaves, refrigerators, medicine cabinets), that data pipeline gets turned back on. That's important because it opens new possibilities for data collection, all kinds of additional biometric data, like what's their emotional state? Has the cadence of their voice changed? Are they manic or are they depressed? We're talking about a significant ecosystem, which in many ways is making our lives easier, but the ways in which that's happening is invisible to us.").

guise of providing convenience to the consumer. In addition to the basic information that is willingly given to Alexa, Amazon also acquires and analyzes recordings of how User X's voice and attitude changed daily in his Interactions. Was he happy, sad, annoyed, calm, or agitated? Now, consider what might happen if User X, an Amazon Prime subscriber, were to attempt to purchase health insurance coverage through Amazon and its "Prime Health" Initiative. Although on his application he might paint himself as an average male living a relatively healthy lifestyle, what is to stop Amazon from employing the information it has already collected on him to determine that his lifestyle and diet put him in a risk category such that his Prime Health insurance premiums would be higher than the average individual or that he might be denied coverage altogether? Under current U.S. data privacy regulations, the unfortunate answer is: absolutely nothing.

Why should consumers care about what happens to their data once it is disclosed to a collector like Amazon? What is the harm? After all, the more that Amazon or a data collector knows about a user, the better the quality of customized, tailored concierge service it can provide. Admittedly, it is difficult to care when the true potential for harm remains unknown; however, this is precisely when the law must step in and proactively protect consumers. Under the current regulatory regime, users and even the data collectors themselves do not always know who is on the receiving end of the information collected or how that information might ultimately be used.[277] As Professor Louis Menand presciently articulated, "[T]he danger of data collection by online companies is not that they will use it to try to sell you stuff. The danger is that that information can so easily fall into the hands of parties whose motives are much less benign."[278] Would users so readily offer personal information if they understood that government agencies like the Drug Enforcement Administration, Internal Revenue Service, and U.S. Customs and Border Protection regularly request, collect, and store

---

277 *See* Louis Menand, *Why Do We Care so Much About Privacy?*, NEW YORKER (June 11, 2018), https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy [https://perma.cc/3V6U-5GCS].

278 *Id.*

information gathered from data collectors?[279] How violated did users feel when their information was unknowingly siphoned by Cambridge Analytica prior to the 2016 election?[280] Absent a comprehensive regulatory regime that prioritizes and safeguards personal data privacy interests, Big Tech and Big Data companies will remain free to exploit the trust and, moreover, the liberty of the average consumer.[281]

C. The Power of Purpose Limitation and Data Minimization

The health insurance hypothetical outlined in Section II.B. above presents a realistic and not-too-distant-future example of how seemingly harmless bits of data collected through Alexa's AI for one purpose might be stored, re-analyzed and re-deployed by Amazon for a completely different purpose, and how such "intangible harms" might harm the consumer.[282] While Amazon has yet to achieve total

---

[279] *See* Alan Henry, *Why You Should Care About and Defend Your Privacy*, LIFEHACKER (Apr. 25, 2012, 11:00 AM), https://lifehacker.com/why-you-should-care-about-and-defend-your-privacy-5904966 [https://perma.cc/2DRR-GAME]; *see also* Saira Hussain & Sophia Cope, *DEEP DIVE: CBP's Social Media Surveillance Poses Risks to Free Speech and Privacy Rights*, EFF (Aug. 5, 2019), https://www.eff.org/deeplinks/2019/08/deep-dive-cbps-social-media-surveillance-poses-risks-free-speech-and-privacy [https://perma.cc/PJL8-TL53].

[280] *See* Kurt Wagner, *Here's How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users*, VOX (Mar. 17, 2018, 3:47 PM), https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data [https://perma.cc/T2RY-3GBK]; *see also* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [https://perma.cc/2BYG-M9Y7]; Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/39XT-B6VD].

[281] *See* Menand, *supra* note 278 (arguing that "privacy" is not what consumers are really worried about, but that the real issue is a curtailment of liberty or the freedom to choose).

[282] For a more positive spin on an example, consultants Debbie Hoffman and Maureen Hydox suggest that:

> Amazon can leverage consumer purchasing data with health information to create a holistic picture of health . . . . Amazon's cloud platform . . . along with their artificial intelligence capabilities could provide physicians with recommendations based on information in the electronic health record (EHR) as well as the consumer's lifestyle based on purchasing patterns and information captured by smart home technologies. These data-based recommendations could identify a

omniscience through an Alexa-controlled data-fueled ecosystem, the repurposing of collected user data is likely already occurring.[283] As Jeff Bezos readily admits, "We never throw away data."[284]

Unfortunately, existing U.S. data privacy laws do little to provide consumers protection from such data repurposing. Amazon's privacy policy contains a section that explains how and with whom the company shares user data.[285] "Subsidiaries of Amazon" are among the recipient list.[286] As such, the consumer, upon creation of her Amazon account, grants Amazon the right to collect her data and consents to its dissemination among Amazon's various divisions and subsidiaries.[287] As the current U.S. privacy regime treats consumer data as an asset of the *company* that collects it rather than of the individual who discloses it, the law would view a user's disclosure to Alexa as voluntary and Amazon's subsequent reuse within its own ecosystem as perfectly legal.[288]

So, the question remains, how should the U.S. legal paradigm shift to better protect the privacy rights of the data subject and ensure that data collected will not harm the subject? One answer lies in the embrace and implementation of two oft-forgotten privacy principles: purpose limitation and data minimization.[289] Although these doctrines have existed as part of the FIPPs since 1973, have

---

> condition and recommend a treatment based on a more holistic look at the consumer's lifestyle, not just their ailment.

Debbie Hoffman & Maureen Hydok, *If Amazon Created a Health System*, HURON (2018), https://www.huronconsultinggroup.com/resources/healthcare/amazon-created-health-system [https://perma.cc/W7XZ-MWAC].

283 *See* Bernard Marr, *Why Data Minimization Is an Important Concept in the Age of Big Data*, FORBES (Mar. 16, 2016, 3:24 AM), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#150d7261da45 [https://perma.cc/73B9-GPVR].

284 *Id.*

285 *See Amazon Privacy Notice*, *supra* note 231.

286 *See id*.

287 *See id*.

288 *See* Naughton, *supra* note 110 (quoting Zuboff's assertion that most data collected becomes "proprietary behavioural surplus").

289 OECD, THE OECD PRIVACY FRAMEWORK 2 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/2K6K-P5C2] [hereinafter OECD FRAMEWORK] ("Organisation for Economic Co-Operation and Development is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation.").

been embraced by the OECD,[290] and have served as the driving forces behind the EU's privacy policies, they have been largely ignored as regulating forces within the United States.[291]

The purpose limitation principle contains two distinct elements: (1) data must only be collected for purposes that are specified (prior to collection), explicit and legitimate; and (2) such data must not be further processed in a way that is incompatible with those purposes.[292] In the event that an entity wishes to employ collected data for a purpose other than that for which it was originally collected, affirmative consent from the user would be required. Purpose limitation returns a degree of control to the user and holds data collectors accountable. It helps to ensure that one's personal data, collected with consent for one purpose (e.g., to affect a financial transaction such as ordering a pizza), would not be indefinitely stored and indiscriminately reused for a different or non-compatible purpose (e.g., to determine eligibility for healthcare coverage).

Data minimization requires that the amount of information collected, used, accessed, or stored be only the *minimum* necessary to achieve the specified purpose.[293] In practice this means that data collectors must limit the collection, storage, and usage of personal data to only that which is relevant, adequate, and essential to accomplish the stated purpose for which the data has been initially processed. According to advocates of the principle, adherence to data minimization not only protects a data subject's privacy interests, but also increases efficiency and reduces risk to the data collector.[294] The less unnecessary data that a company keeps on

---

290 *Id.*

291 *See* Marr, *supra* note 284 (quoting Jeff Bezos: "We never throw away data."). *But see* Jedidiah Bracy, *Apple's New Privacy Push Focuses on Data Minimization*, IAPP (June 9, 2015), https://iapp.org/news/a/apples-new-privacy-push-focuses-on-data-minimization/ [https://perma.cc/3M3R-XMY2] (explaining that Apple has begun to implement data minimization into its designs).

292 *See* OECD FRAMEWORK, *supra* note 290, at 14; *see also* GDPR, *supra* note 141, art. 5(1)(b), at 35.

293 *See* GDPR, *supra* note 141, art. 5(1)(c), at 35.

294 *See* Daniel J. Solove, *The Inquisitive Interrogator: A Data Minimization Story*, TEACHPRIVACY, https://teachprivacy.com/data-minimization-the-inquisitive-interrogator/ [https://perma.cc/9LC5-Z6L5].

hand, the easier and faster it is to locate and employ relevant data.[295] The deletion of data that no longer serves its purpose further limits a company's exposure to breach.[296] Data minimization, therefore, limits the volume of personal information stored by data collectors and further ensures that such personal data cannot be collected, stored, or accessed in perpetuity without affirmative consent from the user.[297]

The two FIPPs principles of purpose limitation and data minimization work in tandem to guarantee that data disclosed by users and collected by brokers remain accurate, relevant, and protected. By embracing these principles alongside those of notice and choice, and implementing them through comprehensive federal data privacy legislation, the current legal paradigm in the United States would shift from one focused on protecting the desires of the tech sector towards one more focused on protecting the information and privacy of the consumer.

D. Proposed Legislative Solutions

The failure of the United States to implement comprehensive federal data privacy reform has created a privacy vortex in which data brokers dominate—dictating a "collect now, decide later" approach to collection—and consumers remain exposed prey to the predatory practices of the tech sector. The current privacy paradigm asymmetrically favors the private tech sector, sanctions dragnet surveillance and leaves data subjects susceptible to financial, emotional, and reputational harm.

---

295 *See id.*

296 *See id.*

297 *See* Marr, *supra* note 284.

1. The States

Despite the recent escalation of hacks,[298] breaches,[299] and egregious exploitation of consumer data by tech companies themselves,[300] the United States still refuses to adopt a more stringent and comprehensive federal data privacy policy. As threats to consumer data privacy increase, the need for comprehensive federal legislation to address these issues intensifies. Unwilling to wait for Congress, and recognizing a need for immediate action, the state legislatures in California, Vermont, and Illinois have taken action to protect their constituents' data privacy.[301] Other states, such as Hawaii, Massachusetts, and New York, have followed the earlier states' lead and thus have similar consumer data privacy legislation pending.[302]

a) California

Unlike the Federal Constitution, California's State Constitution grants its citizens a right of privacy.[303] In keeping with that right, the state had previously enacted privacy legislation that mandates disclosure to users when their data has been breached[304] and demands the provision of clear and conspicuous privacy policies for any business online that collects a California citizen's personal data.[305] In June 2018, California's state legislature passed the California Consumer Privacy Act ("CCPA"), a sweeping privacy

---

298 *See, e.g.*, Joseph Cox, *Hacker Breaches Securus, the Company That Helps Cops Track Phones Across the US*, MOTHERBOARD (May 16, 2018, 1:16 PM), https://motherboard.vice.com/en_us/article/gykgv9/securus-phone-tracking-company-hacked [https://perma.cc/YTQ8-SQKM].

299 *See, e.g.*, Lily Hay Newman, *The Wired Guide to Data Breaches*, WIRED (Dec. 7, 2018, 9:00 AM) https://www.wired.com/story/wired-guide-to-data-breaches/ [https://perma.cc/CTD7-K8RX].

300 *See, e.g.*, Matthew Rosenberg & Sheera Frankel, *Facebook's Role in Data Misuse Sets Off Storms on Two Continents*, N.Y. TIMES (Mar. 18, 2018), https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html [https://perma.cc/C6GC-M27E].

301 *See infra* notes 304–22 and accompanying text.

302 *See infra* notes 323–36 and accompanying text.

303 CAL. CONST. art. 1, § 1.

304 CAL. CIV. CODE §§ 1798.29(a), 1798.82(a) (West 2019).

305 California Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575–22579 (2004).

reform bill that in many ways mirrors the EU's GDPR.[306] The CCPA protects California citizens by embracing the principles of purpose limitation and data minimization, increasing the transparency of data collectors' policies, and providing the consumer with a "right to be forgotten."[307] While the California law enacts substantial protections, its applications reach only as far as California residents.[308] As the law does not take effect until 2020,[309] it remains to be seen what, if any, impact such regulation will have on businesses' treatment of consumers in the remaining forty-nine states.

b) Vermont

In May of 2018, Vermont passed Act 171, which aims to regulate and hold third party data brokers accountable for the sale and misuse of consumers' personal data.[310] The legislation, which took effect January 1, 2019, aims to return some degree of control back to the consumer by attempting to thwart the all-too-common, yet rarely-discussed, practice of shadow profiling—the wholesale collection and subsequent resale of consumer data aggregated from thousands of data points garnered from multiple sources (e.g., browsing history, online purchases, public records, location data[311]) by entities who lack a direct relationship with the consumer.[312] Vermont's legislation compels all third-party data brokers operating in Vermont to be registered with the state,[313] mandates disclosure of

306 CAL. CIV. CODE § 1798.100 (2018).

307 *See id.* §§ 1798.100(a)–(e), 1798.105.

308 *See id.* § 1798.140(g).

309 *See id.*

310 An Act Relating to Data Brokers and Consumer Protection, No. 171, 2018 Vt. Acts & Resolves 584 (codified as VT. STAT. ANN. tit. 9, §§ 2430, 2433, 2446–67, 2480b, 2480h). The act defines "data broker" broadly as "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." VT. STAT. ANN. tit. 9, § 2430(4).

311 *See id.* § 1(a)(1)(B).

312 *See* Katherine E. Armstrong, *Vermont First State to Pass Data Broker Law*, NAT'L L. REV. (June 4, 2018), https://www.natlawreview.com/article/vermont-first-state-to-pass-data-broker-law [https://perma.cc/6HAP-HTGU]; Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers*, TECHCRUNCH (May 27, 2018) https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/ [https://perma.cc/LE4L-T8JT].

313 VT. STAT. ANN. tit. 9, § 2446(a) (West 2019).

collected information pertaining to one's credit scores or report,[314] requires that security protocols be in place to protect the collected data,[315] and imposes steep penalties for violations.[316] While the Vermont law is the first to hold accountable third-party data brokers, it fails to address or hold accountable first-party data brokers (like Amazon).[317] Therefore, businesses that (a) collect data in the natural course of trade, (b) have a direct relationship with the consumer, such as websites, apps, or e-commerce platforms, and (c) do not resell data to third parties are not subject to the law. The law also fails to require consumer consent to the collection or subsequent sale of the data. If the aim of the law is transparency, then affirmative consumer consent—not simply an "opt-out" provision—should be required.

c) Illinois

Although specifically engineered to protect the collection of biometric data (e.g., facial/retina scan, fingerprint, DNA), Illinois' Biometric Information Privacy Act ("BIPA")[318] safeguards the consumer by incorporating the principles of purpose limitation and data minimization.[319] Additionally, BIPA authorizes a private right of action to allow individual consumers to directly sue infringing companies.[320] Lastly, and perhaps most importantly, the courts have interpreted BIPA as a strict liability statute.[321] This means that mere violation of the law is enough to establish a concrete injury that can provide plaintiffs with standing; no other "tangible" harm need be shown to bring a cause of action.[322]

---

314 *Id.* § 2480(b).
315 *Id.* § 2447.
316 *Id.* § 2446(b).
317 *See id.*
318 Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1 (2008).
319 *Id.* § 15(a), (d).
320 *Id.* § 20(1)–(4).
321 *See* Rosenbach v. Six Flags Entm't Corp., 2019 Ill. LEXIS 7, at **17 (Ill. Sup. Ct. 2019).
322 In order to establish Article III standing in the court, a party must adequately allege three elements: (1) an injury in fact (the invasion of a legally protected interest that is (a) concrete and particularized and (b) actual and imminent); (2) a causal connection between the claimed injury and the alleged act(s) of the defendant, such that the injury is fairly traceable to the defendant's act(s) and not the independent action of another third party; and (3) that it is likely, and not merely speculative, that the alleged injury will be redressed

d) Pending State Legislation

Inspired by California's swift passage of CCPA, the state legislatures of Hawaii,[323] Maryland,[324] Massachusetts,[325] Mississippi,[326] Nevada,[327] North Dakota,[328] New Mexico,[329] New York,[330] Rhode Island, [331] and Washington[332] introduced similar comprehensive, omnibus, GDPR-influenced, consumer data privacy legislation at the beginning of 2019. New York also introduced a bill similar to BIPA focused on biometric privacy.[333] The latter half of 2019 saw Mississippi's bill die in committee, New Mexico's bill effectively die with an "action postponed indefinitely" status,[334] and North Dakota's bill reduced to a proposal for a legislative management study.[335] In May 2019, Nevada passed S.B. 220, which amended its current notification law to allow for users to opt out of the sale of their information to third parties. The bill further provides a private right of action for any person injured by a violation of the new right to opt out or the existing obligations to provide notice.[336] The remaining six state bills are pending in various stages of discussion within their respective committees.

---

by a favorable decision. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992). Plaintiffs in data privacy and data breach litigation cases have often struggled with the issue of standing. While a data breach may cause harm, unless that harm resulted in a monetary loss, the injury-in-fact element, where it is concrete and particularized, is difficult to prove. *See also* Priscilla Fasoro & Lauren Wiseman, *Standing Issues in Data Breach Litigation: An Overview*, INSIDE PRIVACY (Dec. 7, 2018), https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview/ [https://perma.cc/NU86-2FSD].

323 S.B. 418, 30th Leg., Reg. Sess. (Haw. 2019).

324 S.B. 613, 2019 Leg., Reg. Sess. (Md. 2019).

325 S.B. 120, 191st Gen. Court, Reg. Sess. (Mass. 2019).

326 H.B. 1253, 134th Leg., Reg. Sess. (Miss. 2019).

327 S.B. 220, 80th Leg., Reg. Sess. (Nev. 2019).

328 H.B. 1485, 66th Leg., Assemb., Reg. Sess. (N.D. 2019).

329 S.B. 176, 54th Leg., 1st Sess. (N.M. 2019).

330 S.B. 224, 2019 Leg., Reg. Sess. (N.Y. 2019).

331 S.B. 234, 2019 Gen. Assemb., Jan. Sess. (R.I. 2019).

332 S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019).

333 S.B. 8547, 2018 Leg., Reg. Sess. (N.Y. 2018).

334 S.B 176, 54th Leg., 1st Sess. (N.M. 2019).

335 H.B. 1485, 66th Leg., Assemb., Reg. Sess. (N.D. 2019).

336 S.B. 220, 2019 Leg., 80th Sess. (Nev. 2019).

e) State Data Breach Notification Statutes

In addition to the pending data privacy statutes mentioned above, all fifty states have also enacted some version of a data breach notification statute, which imposes data protection standards on companies that collect personal information and mandates disclosure protocols when a data breach occurs.[337] While these statutes help inform consumers when their data has been breached, hacked, or stolen, they unfortunately do little to address the way data is collected, to prevent misuse of the collected data, or even to provide courses of action to remedy affected consumers.

2. The Federal Government

In 2015, President Obama proposed a federal privacy bill—the Consumer Privacy Bill of Rights Act—that aimed to give consumers more control over their data and attempted to establish a baseline for the way businesses should treat the collection, storage, and use of consumer data.[338] Although the proposed bill adopted many of the FIPPs—transparency, notice, choice, purpose limitation, and data minimization[339]—it received criticism from privacy advocacy groups as well as the tech sector.[340] The former argued the proposal did not go far enough to protect consumers, while the latter contended such federal regulation was confusing and would stifle innovation.[341] Unfortunately, the plan never gained enough traction in Congress to become law.

---

337 *See* Caleb Skeath & Brooke Kahn, *State Data Breach Notification Laws: 2018 in Review*, INSIDE PRIVACY (Dec. 31, 2018), https://www.insideprivacy.com/data-security/data-breaches/state-data-breach-notification-laws-2018-in-review/ [https://perma.cc/H7YN-2JF7].

338 *See* WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 (proposed Feb. 27, 2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/3PYW-GN8Q] (currently before the Committee on the Judiciary). The discussion draft differs substantively from the Bill that ultimately went to the Senate. *See* Consumer Privacy Bill of Rights Act of 2015, S. 1158, 114th Cong. (2015).

339 *See id.* §§ 101–04.

340 *See* Brendan Sasso, *Obama's 'Privacy Bill of Rights' Gets Bashed from All Sides*, ATLANTIC (Feb. 27, 2015), https://www.theatlantic.com/politics/archive/2015/02/obamas-privacy-bill-of-rights-gets-bashed-from-all-sides/456576/ [https://perma.cc/UJ5S-KDVN].

341 *See id.*

More recently, however, several Senators, including Brian Schatz (D-HI), Mark Warner (D-VA) and Edward Markey (D-MA), have drafted federal data privacy proposals for Senate consideration. Senator Schatz's Data Care Act of 2018 borrows from Jack Balkin's theories and aims to establish a fiduciary relationship between data brokers and data subjects.[342] His bill would impose fiduciary duties of care, loyalty, and confidentiality onto data brokers to ensure that collected data could not be used in a manner that would bring harm to the data subject. Senator Warner's DETOUR Act also embraces the idea of imposing fiduciary duties upon data collectors, but focuses more on regulating predatory design elements such as the user interface and the algorithmic equations that siphon data.[343] Warner's bill recommends heightening the standard of transparency for algorithms that govern data collection, expanding and empowering the FTC to become the official privacy regulator, and adopting GDPR-like structures to protect data subjects.[344]

Senator Markey's Privacy Bill of Rights Act eschews the problematic information fiduciary construct[345] and instead proposes a return to the FIPPs and the empowerment of the individual user.[346] In doing so, however, Markey's bill suggests a loose framework—including the principles of purpose limitation and data minimization as well as affirmative "opt-in" consent—but does not actually pass any regulation at all. Instead, it shifts the onus for such regulation to the FTC to promulgate rules that comport with the ideals set forth in his legislation.[347]

To date, each of the federal legislative proposals has been introduced or is currently under consideration in its respective committee.[348] However, none has garnered the bipartisan or tech

---

342 *See* Data Care Act of 2018, S. 3744, 115th Cong. (2018).

343 *See* Deceptive Experiences To Online Users Reduction Act, S. 1084, 116th Cong. (2019)

344 *See id.*

345 *See* Kahn & Pozen, *supra* note 126 (arguing that the imposition of fiduciary duties on data collectors creates a conflict with the fiduciary duties already owed shareholders and thus, a legally untenable paradigm).

346 *See* Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019).

347 *See id.* §§ 3–4.

348 *See Congressional Chronicle*, C-SPAN, https://www.c-span.org/congress/bills/bill/?116/s1214 [https://perma.cc/T4UQ-FNAZ] (status: introduced); *id.*, https://www.c-span.

sector support necessary to achieve passage. Moreover, while each proposal contains a noteworthy or important element that attacks a particular issue of data privacy or data protection, no singular piece of legislation has presented the kind of comprehensive, omnibus reform necessary to address the rising threats posed by the rapid advancement of data collection technology via AI.

IV. MOVING FORWARD: A HYBRID PROPOSAL FOR THE FUTURE

Today, the technology of AI, the internet, and the IoT transcends the previous constraints of physical or geographic boundaries. Big Data collectors such as Amazon now operate in an interconnected global economy where data functions as the prime currency.[349] The current threats posed to consumer data privacy by unregulated tech entities cannot be mitigated by a disparate patchwork of localized, state, or sectoral solutions. The only way to effectively and efficiently curtail these privacy risks is to pass comprehensive, federal consumer data privacy legislation that will impose restrictions on the collection of personal data regardless of the sector or entity collecting, establish baselines for acceptable collection practices, outline prohibitions for the collection, storage, and usage of personal data, and uniformly enforce penalties for violations across all fifty states.

Given the pace at which data collection technology continues to advance and the exponential growth of the tech sector's thirst to exploit such collected data, the current self-regulatory regime can no longer be sustained. The government must intervene. However, for federal legislation to be effective and efficient in regulating entities and protecting the consumer from predatory data collection, retention, and use, it must address several key elements.

---

org/congress/bills/bill/?116/s1084 [https://perma.cc/3NFT-CYU3] (status: introduced); *id.*, https://www.c-span.org/congress/bills/bill/?115/s3744 [https://perma.cc/7MW9-G3X8] (status: stalled in committee).

[349] *See The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/QWB9-48JT].

A. A Return to the FIPPs and the Establishment of a Consumer Privacy Bill of Rights

One of the main focuses for new federal legislation must be to allow consumers to reclaim and retain control of their data. Due to the failure of "Notice and Choice," consumers have only the illusion of control; however, once they consent to engage with a company, any control over their data subsequently resides in the hands of the data collectors and not the data subjects.[350] To empower and protect the consumer, therefore, federal legislation must shift the privacy paradigm away from dependence solely on "Notice and Choice" and towards a regime that adopts all of the FIPPs, including the key principles of purpose limitation and data minimization,[351] as outlined by the OECD[352] rather than the FTC.

The full array of FIPPs—including purpose limitation and data minimization—must be incorporated and codified into a federal Consumer Bill of Rights, which would comprehensively outline the freedoms bestowed upon and powers granted to the consumer across all fifty states. Borrowing aspects from the GDPR[353] and Obama's original 2012 privacy proposal,[354] the Bill of Rights should establish a baseline for consumer data protection and demand that data collectors provide users with the transparency necessary to identify, access, interrogate, correct and delete all collected information. All such rights should be applied not only proactively but also retroactively, so that data collected prior to legislation would be subject to the same restrictions and regulations.

B. A Dedicated Privacy Regulatory Body

Congress has never delegated privacy oversight to any regulatory body; therefore, new federal legislation must rectify this previous omission. Since the FTC has become the de facto privacy

---

350 *See supra* Section III.A.

351 *See supra* Section III.B.

352 The FIPPs under the OECD include principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. *See* OECD Framework, *supra* note 290.

353 *See* GDPR, *supra* note 141, ch. 3, at 39–47.

354 *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK OF PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 10 (2012).

regulator,[355] it seems most efficient to keep oversight under their auspices. However, in doing so, it is further imperative to create a dedicated data privacy division within the larger federal agency that is adequately staffed, funded, and endowed with the full range of regulatory tools necessary to effectively and efficiently enforce the more-robust data privacy laws that this Note envisions. This means that full rulemaking authority under Section 553 would need to be restored for privacy oversight; thus, the restrictive amendments of Moss–Magnuson and the FTC Improvement Act should be repealed for data privacy regulations. Additionally, any FTC-led regulatory body would need to have the ability to prosecute all federal data privacy violations as well as any violations of Section 5 of the FTC Act.

C. Civil Right of Action

Much of the legislation that has been proposed at the state and federal level focuses on government-based action against private sector statutory violations. However, a crucial element that should be included in any future data privacy legislation is a civil right of action, which may be triggered by a mere violation of a statutory provision.[356] The creation of a strict liability regime for data privacy violations would allow victims of predatory data practices a means by which to seek judicial redress. Without it, consumers who have suffered at the hands of Big Data and Big Tech would likely not be able to bring tech companies to court.[357] The inclusion of a strict liability civil right of action would allow consumers to demonstrate a concrete harm and would eliminate the issues of standing that have previously crippled plaintiffs who have attempted to bring civil suits against companies for data breaches.[358] To make recovery easier for the consumer and to limit the litigation costs for violative data collectors, a civil right of action provision could also include tiered statutory damages depending on the magnitude of the breach.

---

355 *See supra* Section II.D.

356 *See, e.g.*, Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1 (2005).

357 *See* discussion *supra* note 323.

358 For a more detailed explanation of this issue, see *supra* note 257.

D. State Law Preemption

Comprehensive federal privacy legislation must also address the contentious issue of state law preemption. Since the passage of the CCPA, California representatives Jackie Spier and Ro Khanna have been vocal in their opposition to the potential preemption of their state's comprehensive privacy law by federal legislation.[359] They remain concerned that federal legislation will create a less stringent framework for consumer privacy protection. If Congress adequately addresses the issues currently plaguing consumers—issues that have already been addressed by several state bills[360]—then preemption should become a non-issue. However, if Congress punts and passes a bill that fails to solve the holistic problem identified by this Note, then states will rightfully see a need to step in to more fully protect their constituents. Therefore, to avoid these issues, a federal bill should use the structure and thresholds established by the CCPA (or other comprehensive state laws) as a baseline or "floor" for any legislation. If the aim is to create a uniform set of rules for the tech sector to follow across all fifty states, the federal bill should be no less stringent or exacting than any current state bill. However, in the event that the federal bill passes with less exacting measures than current state laws, states must be permitted to enact stricter legislation to fill the gaps.

E. The Promotion of Innovation

Finally, although comprehensive data privacy reform should primarily focus on the protection of the consumer from predatory practices, it is crucial that any legislation in this area maintains ample space to allow the tech sector to continue to innovate, expand, and foster competition. Although the era of self-regulation must come to an end, any regulatory regime will have far more success working *with* the entities regulated rather than working *against* them.

---

[359] *See* Cristiano Lima & John Hendel, *California Democrats to Congress: Don't Bulldoze Our Privacy Law*, POLITICO (Feb. 21, 2019, 5:07 AM), https://www.politico.com/story/2019/02/21/congress-data-privacy-california-1185943 [https://perma.cc/SH4Y-ACDB].

[360] *See supra* Section III.D.1.

CONCLUSION

As the manipulation of Big Data continues to produce big profits, the threats to consumer data privacy continue to escalate. Today, thanks to Amazon's ubiquitous Alexa and other smart assistants, the data collection capabilities of AI have infiltrated the most personal spheres of its users such as the home. It is only a matter of time before AI dominates other traditionally "protected" spaces such as our cars,[361] our businesses,[362] and our classrooms.[363] Although the innovations of the tech sector need not be stifled simply because consumers desire data privacy protection, the tech sector can no longer be permitted to run roughshod over consumers' rights under the guise of progress. The United States' patchwork sectoral regime of the past must give way to comprehensive reform for the future. Congress can and should work to implement comprehensive protections to consumer data privacy that will increase transparency, minimize predatory collection, storage and use practices, and empower the individual consumer over the tech industry. The clocks cannot be turned back, nor can data already collected necessarily be returned. However, by passing comprehensive legislation that will institute a uniform system of federally mandated rules and regulations, the government can begin to protect the autonomy, reputation and financial security of the consumer and safeguard the personal data privacy rights of the individual.

---

361 *See* Stephen Edelstein, *Amazon Alexa Can Now Hitch a Ride in Any Car with Echo Auto*, DIGITAL TRENDS (Sept. 21, 2018, 7:07 AM), https://www.digitaltrends.com/cars/amazon-echo-auto/ [https://perma.cc/9V3Q-HSLN]; *see also Echo Auto—The First Echo for Your Car*, AMAZON, https://amzn.to/2V7Cqpz [https://perma.cc/2J4X-JTNL].

362 *See* Vaughn Highfield, *Amazon Alexa for Business Is Coming to Your Office in a Big Way*, ALPHR (Oct. 25, 2018), https://www.alphr.com/amazon/1010095/amazon-alexa-for-business-is-coming-to-your-office-in-a-big-way [https://perma.cc/Y9FS-WJC4]; Emily Price, *Amazon Is Allowing Companies to Make Office-Specific Alexa Apps*, FORTUNE (Mar. 29, 2019), http://fortune.com/2019/03/29/amazon-is-allowing-companies-to-make-office-specific-alexa-apps/ [https://perma.cc/J5KG-P47U]; *see also Alexa For Business*, AMAZON, https://aws.amazon.com/alexaforbusiness/ [https://perma.cc/4V4D-MD4N].

363 *See* Matthew Lynch, *Using Amazon Alexa in the Classroom*, TECH EDVOCATE (Mar. 15, 2018), https://www.thetechedvocate.org/using-amazon-alexa-classroom/ [https://perma.cc/Q6R4-UNVU]; *see also* Marrian Zhou, *Amazon's Alexa Is Going to College*, CNET (Aug. 16, 2018), https://www.cnet.com/news/amazons-alexa-is-going-to-college/ [https://perma.cc/JCJ7-7ZSN].