Oklahoma Law Review

Volume 74 | Number 4
A Life's Work: In Memory of Professor Jonathan B. Forman

2022

Bringing Down Big Data: A Call for Federal Data Privacy Legislation

Madeline M. Cook

Bringing Down Big Data: A Call for Federal Data Privacy Legislation

Table of Contents

Introduction

The concept of online privacy is entirely an illusion. Imagine that last night, while watching a show on Netflix, you decided that you wanted to buy a new couch. You paused the show to share the idea with your partner, and after a short conversation, you agreed to go sofa shopping that weekend. You then finished your episode and went straight to bed. This morning, as you scroll through Facebook,[1] the very first advertisement you see is for a sofa from a brand you have never heard of. It is exactly what you pictured last night. But how did Facebook know that? Before this morning, Facebook had never shown you an ad for furniture. You had not yet begun sofa shopping online. You did not even know that you wanted a new couch until last night. The only way Facebook could have known you wanted to buy a new couch would be if it had eavesdropped on your conversation with your partner the night before. But Facebook was not listening.[2]

This phenomenon is such a widely shared experience among Facebook users that it has become a popular conspiracy theory.[3] Facebook explicitly

1. On October 28, 2021, Facebook changed its corporate name to Meta. Mike Isaac, *Facebook Renames Itself Meta*, N.Y. TIMES (Oct. 28, 2021), https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html. While Mark Zuckerberg, the company's chairman and CEO, announced that the change marked a shift in focus away from social networking and toward developing "metaverse" technologies, critics see the move as a largely "cosmetic" attempt to distance the company from recent bad press involving its data practices and content policies. *See id.* Because this Comment was written around the same time as the name change and relies on sources that refer to both the social media giant and its parent company as "Facebook," there is a risk that references to the company may not always clearly denote which is being discussed. For the purposes of consistency, however, this Comment uses the name Facebook for all references to the company both pre- and post-name change, except to the extent that a source specifically refers to the company as Meta.

2. *See Facebook Does Not Use Your Phone's Microphone for Ads or News Feed Stories*, META (June 2, 2016) [hereinafter *Facebook Does Not Use Your Phone's Microphone*], https://about.fb.com/news/h/facebook-does-not-use-your-phones-microphone-for-ads-or-news-feed-stories/.

3. *See* Reply All, *#109 Is Facebook Spying on You?*, GIMLET (Nov. 2, 2017), https://gimletmedia.com/shows/reply-all/z3hlwr; *see also* Ben Gilbert, *There's a Wildly Popular*

addressed the theory in 2016, saying that it "does not use your phone's microphone to inform ads or to change what you see in News Feed,"[4] but many people were left unconvinced.[5] Even if Facebook does not show ads based on what people say aloud,[6] it spies on users in an equally intrusive way.

Although you did not search for a couch last night, your Facebook-using partner did. At some point while browsing for furniture, your partner accessed a website with an ad tracker installed. Nearly four in five websites host at least one ad tracker,[7] and some host as many as fifty.[8] Facebook Pixel (Facebook's ad tracker) is a piece of code installed on millions of websites[9] that watches everything a person does on a website and reports the data back to Facebook.[10] Through powerful algorithms, Facebook builds out shadow profiles for individuals based on this data and lets companies access this data to "actively target individuals who might be interested in [the companies'] products."[11]

When your partner clicked on a Facebook Pixel-monitored website and perused the sofa section, Facebook learned they were interested in buying a couch. Because Facebook knew that you lived together—through a combination of willingly and unwillingly shared location data[12] and

---

Conspiracy Theory That Facebook Listens to Your Private Phone Calls, and No Matter What the Tech Giant Says, People Just Aren't Convinced It's Not True, INSIDER (Aug. 14, 2019, 10:05 AM), https://www.businessinsider.com/facebook-ads-listening-to-you-2019-5.

4. *Facebook Does Not Use Your Phone's Microphone*, *supra* note 2.

5. *See* Gilbert, *supra* note 3.

6. *See Facebook Does Not Use Your Phone's Microphone*, *supra* note 2.

7. Nicole Lindsey, *Invasion of Privacy: Tracking Your Online Behavior Across the Web*, CPO MAG. (Dec. 6, 2017), https://www.cpomagazine.com/data-privacy/invasion-of-privacy-tracking-online-behavior-across-web/.

8. Several journalists have documented that websites like the *New York Times* can have anywhere from thirty to fifty different companies' trackers attached to a single article. *See* Reply All, *supra* note 3, at 06:57 (noting that the *New York Times* website hosts approximately thirty to forty ad trackers); Timothy Libert, Opinion, *This Article Is Spying on You*, N.Y. TIMES (Sept. 18, 2019), https://www.nytimes.com/2019/09/18/opinion/data-privacy-tracking.html (noting that nearly fifty different ad trackers were attached to a *New York Times* article about abortion).

9. *See* Reply All, *supra* note 3, at 06:10.

10. *Id.*

11. *See Advanced Targeting Strategies for Performance Marketers*, FACEBOOK BUS., https://www.facebook.com/business/a/performance-marketing (last visited Jan. 7, 2022).

12. *See* Chris Smith, *Facebook Tracks Your Location Even If You Think You Opted Out*, BGR (Dec. 19, 2018, 9:26 AM), https://bgr.com/2018/12/19/facebook-location-tracking-features-how-facebook-tracks-you-for-ads/ (explaining that even when people opt out of sharing their location data from their smartphones, Facebook uses its data about people's "browsing habits, including IP address, Wi-Fi network, and Bluetooth to pinpoint [their]

information you voluntarily posted on your Facebook profile—it strategically served you an ad for the couch your partner discovered the night before.[13]

Even if you are not one of Facebook's 2.94 billion monthly active users on the company's main platform,[14] Facebook, Google, and other large technology companies still harvest your data.[15] Facebook and Google even have data profiles for people who have never signed up for the companies' services.[16] Google in particular has recorded enough data about you to fill three million Word documents.[17] It knows everything you have ever searched for or deleted, every website you have clicked on, and every location where you have turned on your phone.[18] If you are one of the 2.5 billion monthly active users of an Android mobile operating system,[19] your phone pulls data from you over one hundred thousand times a day, often when your screen is blank, and Google and Facebook ping your location data six thousand times a day.[20] Every YouTube video you have ever watched, Google has watched along with you.[21] It has read every email you have sent, received, or deleted.[22] And this surveillance carries across all of your devices.[23]

Pervasive digital surveillance is the industry standard for technology giants like Facebook, Google, Amazon, and Microsoft ("Big Tech").[24] Yet

whereabouts and place relevant ads inside its apps. And all of this happens as Facebook continues to give users the impression they can control whether or not they share location data with Facebook.").

13. *See generally* Reply All, *supra* note 3.

14. *See Facebook Stats and Trends*, DATAREPORTAL (May 11, 2022), https://datareportal.com/essential-facebook-stats.

15. AMNESTY INT'L, SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS 40 (2019) [hereinafter SURVEILLANCE GIANTS], https://www.amnesty.org/en/documents/pol30/1404/2019/en/.

16. *See id.* at 12.

17. Dylan Curran, *Are You Ready? Here Is All the Data Facebook and Google Have on You*, GUARDIAN (Mar. 30, 2018, 3:17 EDT), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

18. *See id.*

19. *See* David Curry, *Android Statistics (2022)*, BUS. APPS (May 4, 2022), https://www.businessofapps.com/data/android-statistics/.

20. Chris Hoofnagle, *Facebook and Google Are the New Data Brokers*, DIGIT. LIFE INITIATIVE (Jan. 5, 2021) [hereinafter Hoofnagle, *Facebook and Google*], https://www.dli.tech.cornell.edu/post/facebook-and-google-are-the-new-data-brokers.

21. *See* Curran, *supra* note 17.

22. *Id.*

23. *See* SURVEILLANCE GIANTS, *supra* note 15, at 12.

24. *See id.* at 10.

even the basics of how these companies' data models and "black box"[25] algorithms function remain shrouded in secrecy. They are kept from the public through non-disclosure and non-disparagement agreements[26] and trade secret protection.[27] Even within the companies, artificial intelligence and machine learning render the inner workings of these companies' algorithms unknowable.[28] Worst of all, these algorithms influence our lives, dictating the information, ideas, opinions, and products we are exposed to online. These companies allow us to communicate, collaborate, share, discover, learn, create, and physically navigate the world through their "free" services, but the services they provide are not free. In modern society, personal data is currency, and we are paying a very high price.

This Comment explores how social media and technology companies, data brokers, and other actors exploit the data of every U.S. citizen and calls for a comprehensive federal data privacy regulatory framework. Part I contextualizes the problem, exploring how and why companies collect data and how they profit from this business model. Part II investigates how these companies' data practices are detrimental to the fabric of society, explaining how consumers lack the ability to consent to data collection, how companies and other (often bad) actors use this data for large-scale manipulation, and how, in doing this, companies are contributing to violations of the human right to privacy. Part III compares existing and proposed privacy laws from around the country and the globe. Finally, Part IV suggests how U.S. policymakers should approach the task of creating a federal data privacy law, highlighting the necessity for both a sweeping federal framework and the creation of a new federal agency to enforce it.

I. The History of the Big Data Business

While Google and Facebook have received attention for the ways they collect and monetize their troves of user data, they were not the first companies to do so, nor are they the only ones engaging in these practices.

---

25. *See* Dallas Card, *The "Black Box" Metaphor in Machine Learning*, MEDIUM (July 5, 2017), https://dallascard.medium.com/the-black-box-metaphor-in-machine-learning-4e57a3a1d2b0 ("The black box metaphor dates back to the early days of cybernetics and behaviourism, and typically refers to a system for which we can only observe the inputs and outputs, but not the internal workings.").

26. *See* Hoofnagle, *Facebook and Google*, *supra* note 20.

27. Marietje Schaake, *Trade Secrets Shouldn't Shield Tech Companies' Algorithms from Oversight*, BROOKINGS (May 4, 2020), https://www.brookings.edu/techstream/trade-secrets-shouldnt-shield-tech-companies-algorithms-from-oversight/.

28. THE SOCIAL DILEMMA, at 48:17 (Netflix 2020).

To fully appreciate the need for a comprehensive federal data privacy law, it is essential to understand who collects our data, how they do it, and why it is worth so much money. This Part explores the evolution of surveillance-based business models beginning with data brokers and ending with social media and other Big Tech companies.

A. Data Brokers

Before Big Tech was involved in the Big Data industry, data brokers reigned supreme. There is a $227-billion-per-year industry dedicated to buying and selling consumer data.[29] Data brokers are "companies that collect consumers' personal information"[30] from a plethora of online and offline sources, both publicly available and not, and share or resell this information to others.[31] Importantly, data collection almost always happens without the consumer's knowledge or consent. The most basic information that is harvested usually includes a person's name, age, sex, address, telephone number, email addresses, voter registration, and social security number.[32] But these companies also know your income,[33] whether you have been divorced,[34] the ages and sexes of your children,[35] your web browsing history,[36] your consumer purchase data,[37] and the size of your house "within twenty-five square feet."[38] Data brokers often run the loyalty programs at big-box stores, supermarkets, and pharmacies.[39] This means that if you have

29. *See* Daniel Newman, *Apple, Meta and the $10 Billion Impact of Privacy Changes*, FORBES (Feb. 10, 2022, 7:40 PM EST), https://www.forbes.com/sites/danielnewman/2022/02/10/apple-meta-and-the-ten-billion-dollar-impact-of-privacy-changes/?sh=1fcb132272ae.

30. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i (2014) [hereinafter FTC, DATA BROKERS], https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

31. Michal Wlosik, *What Is a Data Broker and How Does It Work?*, CLEARCODE (Aug. 19, 2021), https://clearcode.cc/blog/what-is-data-broker/.

32. *Id.*; *see* FTC, DATA BROKERS, *supra* note 30, at iv.

33. Reply All, *supra* note 3, at 08:34; *see* Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014, 1:50 PM EDT), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

34. *See* Reply All, *supra* note 3, at 08:29.

35. *See* Beckett, *supra* note 33 (discussing how Disney sold this data to other companies).

36. FTC, DATA BROKERS, *supra* note 30, at iv.

37. *Id.*

38. Reply All, *supra* note 3, at 08:23.

39. *See id.* at 08:36; *see also* Beckett, *supra* note 33 ("Datalogix, for instance, which collects information from store loyalty cards, says it has information on more than $1 trillion in consumer spending 'across 1400+ leading brands.'").

ever signed up for a store loyalty program, "they know how often you're buying diapers, or cold medicine, or birth control."[40] From this data, data brokers infer a consumer's interests and use those interests to sort them into hyper-specific categories.[41]

Some of the relatively mundane categories include "Winter Activity Enthusiast" and "Dog Owner."[42] Other, more problematic categories "include those that primarily focus on ethnicity and income levels, such as 'Urban Scramble' and 'Mobile Mixers,'" which are composed of high concentrations of low-income Black and Hispanic people.[43] Shockingly, data brokers have even posted lists for sale titled "Rape Sufferers List," "'erectile dysfunction sufferers,' 'alcoholism sufferers' and 'AIDS/HIV sufferers.'"[44] These lists are sold to a wide variety of entities including businesses, advertisers, other data brokers, and insurance companies.[45] Some data brokers have even "custom-tailored" their websites to sell data to law enforcement agencies.[46]

In December 2021, the Center for Democracy and Technology reported a troubling finding: While law enforcement and intelligence agencies use terms like "open source" and "publicly available" to describe the information they purchase from data brokers, in reality the government is often purchasing sensitive information about individuals' private "communications, finances, health, [and] patterns of travel."[47] This becomes

---

40. Reply All, *supra* note 3, at 08:43.

41. *Id.* at 09:00; FTC, DATA BROKERS, *supra* note 30, at iv–v.

42. FTC, DATA BROKERS, *supra* note 30, at 47.

43. *Id.*

44. Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers,'* FORBES (Dec. 19, 2013, 3:40 PM EST), https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/?sh=664eaed51d53. In December 2013, Pam Dixon, a privacy expert, testified to Congress that she had found those lists for sale from data brokers. *Id.*

45. *See* GINA MARIE STEVENS, CONG. RSCH. SERV., RS22137, DATA BROKERS: BACKGROUND AND INDUSTRY OVERVIEW 3 (2007), https://www.everycrsreport.com/files/20070503_RS22137_df01b0feeaa88a3849662fabab83d5ff32cd8762.pdf.

46. *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. 595, 596 (2003); *see also* STEVENS, *supra* note 45, at 3.

47. *See* Sharon Bradford Franklin & Dhanaraj Thakur, *New CDT Report Documents How Law Enforcement & Intel Agencies Are Evading the Law and Buying Your Data from Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 9, 2021), https://cdt.org/insights/new-cdt-report-documents-how-law-enforcement-intel-agencies-are-evading-the-law-and-buying-your-data-from-brokers/.

especially troubling in light of the Supreme Court's recent decision in *Dobbs v. Jackson Women's Health Organization*,[48] which overruled *Roe v. Wade*[49] and *Planned Parenthood v. Casey*.[50] Already, states like Oklahoma and Texas have passed laws that criminalize abortion[51] and allow private citizens to recover civil damages "from anyone who helps someone get an abortion."[52] This means that not only state law enforcement agencies, but also private individuals, suddenly have an interest in who might be traveling to or from abortion clinics around the country. The danger here is not speculative. A company called SafeGraph, which in 2021 sold the location data of millions of Americans to the Centers for Disease Control and Prevention (which was interested in tracking citizens' compliance with curfews and stay-at-home orders during the COVID-19 pandemic),[53] also sells location data for people who visit abortion clinics.[54] For just $160, a *Vice* reporter was able to purchase location data for every person who visited any of Planned Parenthood's more than six hundred clinics over the course of a week.[55] Included in this data set was not only information about how long people stayed at the clinics, but also where they traveled before and after their visits.[56]

There are hundreds of different data brokers[57] operating in the United States that collect different types of data on individuals.[58] Some of the more

48. 142 S. Ct. 2228 (2022).

49. 410 U.S. 113 (1973).

50. 505 U.S. 833 (1992).

51. *See* Jordan Smith, *Oklahoma's Total Abortion Ban Will Mean Surveillance, Criminalization, and Chaos*, INTERCEPT (May 20, 2022, 11:15 AM), https://theintercept.com/2022/05/20/oklahoma-abortion-ban-surveillance-criminalization/.

52. Elaine Kamarck, *The Supreme Court's Abortion Decision—Just the Beginning of the Battle*, BROOKINGS (June 24, 2022), https://www.brookings.edu/blog/fixgov/2022/06/24/the-supreme-courts-abortion-decision-just-the-beginning-of-the-battle/.

53. Joseph Cox, *CDC Tracked Millions of Phones to See if Americans Followed COVID Lockdown Orders*, VICE (May 3, 2022, 8:00 AM), https://www.vice.com/en/article/m7vymn/cdc-tracked-phones-location-data-curfews.

54. *See* Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022, 11:46 AM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

55. *Id.*

56. *Id.*

57. Julia Angwin, *Privacy Tools: Opting Out from Data Brokers*, PROPUBLICA (Jan. 30, 2014, 1:29 PM EST) [hereinafter Angwin, *Privacy Tools*], https://www.propublica.org/article/privacy-tools-opting-out-from-data-brokers (highlighting how Julia Angwin, a technology journalist for *ProPublica*, identified 212 individual data brokers).

58. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 68 (2012) [hereinafter

well-known companies include Acxiom, Datalogix, Equifax, Experian, and LexisNexis.[59] In a 2012 report about protecting consumer privacy, the Federal Trade Commission ("FTC") sorted data broker companies into three categories: "(1) entities subject to the FCRA [Fair Credit Reporting Act]; (2) entities that maintain data for marketing purposes; and (3) non-FCRA covered entities that maintain data for non-marketing purposes that fall outside of the FCRA, such as to detect fraud or locate people."[60]

The FCRA is a 1970 statute regulating companies' provision of consumer data when it is used or might be used to make decisions about a person's eligibility for credit, insurance, housing, and employment, as well as other eligibility determinations.[61] The motivation behind the FCRA was policymaker concern about "the lack of transparency among companies" dealing in such data.[62] Importantly, the FCRA does not apply to the use or sale of consumer data for marketing purposes.[63] This means that, while U.S. citizens have the right to review and correct their credit reports, "there's often no way to know" the exact information a marketing or other kind of data broker knows about an individual or whether such information is correct.[64]

Despite decades-long policymaker concern "about the lack of transparency of companies that buy and sell consumer data without direct consumer interaction,"[65] and repeated reports by the FTC calling for regulation of the other categories of data brokers,[66] these businesses have been left unregulated. This has led to a world in which Acxiom, a data broker that "provides consumer data and analytics for marketing campaigns and fraud detection," has "over 3000 data segments for nearly every U.S. consumer."[67] A subsidiary of Equifax, a credit reporting data broker, "even collects detailed salary and pay stub information for roughly 38 percent of

---

FTC, PROTECTING CONSUMER PRIVACY], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

59. *See* Angwin, *Privacy Tools*, *supra* note 57.

60. FTC, DATA BROKERS, *supra* note 30, at i (citing FTC, PROTECTING CONSUMER PRIVACY, *supra* note 58, at 65).

61. *Id.*

62. *Id.*

63. *See id.*

64. *See* Beckett, *supra* note 33. *See generally id.* (discussing the lack of transparency in data broker practices and difficulty consumers experience in correcting inaccurate information).

65. FTC, DATA BROKERS, *supra* note 30, at i.

66. *See* FTC, PROTECTING CONSUMER PRIVACY, *supra* note 58, at i–ii, v.

67. FTC, DATA BROKERS, *supra* note 30, at 8.

employed Americans."[68] In 2010, Josh Nardone, a chief executive for an undisclosed data broker, told the Wall Street Journal, "We never don't know anything about someone."[69]

These categories, lists, and data points do not only exist in a vacuum on data brokers' servers; they have real-world implications. In 2014, "Office Max sent a letter to a grieving father addressed to his name, followed by 'daughter killed in car crash.'"[70] Retailers, including Staples, Office Depot, Rosetta Stone, Home Depot, and Discover Financial Services, have used aggregated data about user characteristics to "consistently adjust[] prices and display[] different product offers" on their websites.[71] For Office Depot, these characteristics include a customer's geolocation and browsing history.[72] Capital One Financial Corporation even uses individual consumer data to "instantly decide which credit cards to show first-time visitors to its website."[73]

While some might argue that companies can utilize these types of consumer date to create a more personalized, and therefore desirable, online shopping experience, that is not always the case. The data is often wrong.[74] When Caitlyn Renee Miller, a journalist for *The Atlantic*, paid fifty dollars for a report from one data broker, nearly 50% of the information about her was incorrect.[75] And when Julia Angwin, an investigative journalist and former senior reporter at *ProPublica*, requested reports from several data brokers, she was "equally irked by the reports that were wrong . . . as [she] was by the ones that were correct."[76] While most data brokers will share some

68. Beckett, *supra* note 33.

69. Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J. (Aug. 4, 2010) [hereinafter *On the Web's Cutting Edge*], https://www.wsj.com/articles/SB10001424052748703294904575385532109190198.

70. Beckett, *supra* note 33.

71. Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

72. *Id.*

73. *On the Web's Cutting Edge*, *supra* note 69.

74. *See* Caitlyn Renee Miller, *I Bought a Report on Everything That's Known About Me Online*, ATLANTIC (June 6, 2017), https://www.theatlantic.com/technology/archive/2017/06/online-data-brokers/529281/; *see also* Angwin, *Privacy Tools*, *supra* note 57; *On the Web's Cutting Edge*, *supra* note 69.

75. *See* Miller, *supra* note 74.

76. Angwin, *Privacy Tools*, *supra* note 57.

data with consumers who may have to jump through hoops to request it,[77] brokers only provide consumers access to some of the data and inferences made about them.[78] And even then, the data is typically provided to the consumer in a raw format, meaning that consumers may not be able to identify what categories they have been sorted into, even with the data in their hands.[79]

Most troublingly, it is extremely difficult, if not impossible, for most consumers to stop data brokers from collecting and distributing their data.[80] This process is called opting out, which "means suppressing the consumer's personal information from display in the data broker's marketing products."[81] In 2014,[82] Julia Angwin tried to opt out of data brokers' collection and distribution of her data.[83] She identified 212 brokers, and of those, "less than half—92—accepted opt-outs. Of those, a majority—65—required [her] to submit some form of identification," like a driver's license or social security number to opt out.[84] While many companies allow for an opt-out request to be submitted online,[85] twenty-four of the companies Angwin identified "required the opt-out forms to be sent by mail or fax."[86] While some companies have taken steps to enable consumers to more easily access and even correct some of their personal data,[87] most companies only did so after

77. *See* FTC, DATA BROKERS, *supra* note 30, at 42 ("These data brokers provide notice on their website, typically within a lengthy privacy policy, and an explanation of how to access the information; however, these notices may be hard to understand.").

78. *Id.*

79. *Id.*

80. Beckett, *supra* note 33.

81. FTC, DATA BROKERS, *supra* note 30, at 42–43.

82. At the time of her article's publication, there was no law that required data brokers to even offer opt-outs. *See* Angwin, *Privacy Tools*, *supra* note 57. Since her 2014 experiment, California has passed laws that require data brokers to allow their respective citizens the right to opt out of data collection. *See What Are Data Brokers Required to Do Under California Law?*, BCLP LAW (July 9, 2020), https://www.bclplaw.com/en-US/insights/what-are-data-brokers-required-to-do-under-california-law.html. Vermont has also passed a law that "requires companies to spell out whether there's any way for consumers to opt out of their data collections." Steven Melendez, *A Landmark Vermont Law Nudges over 120 Data Brokers Out of the Shadows*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90302036/over-120-data-brokers-inch-out-of-the-shadows-under-landmark-vermont-law. For more discussion about state laws requiring companies to allow users to opt out of data collection, see *infra* Section III.C.

83. Angwin, *Privacy Tools*, *supra* note 57.

84. *See id.*

85. *See id.*

86. *Id.*

87. *See* FTC, DATA BROKERS, *supra* note 30, at 42.

they were forced to change their data practices for some Americans in response to recent state legislation.[88] Despite the FTC's persistent recommendations, there remains no federal law beyond the FCRA regulating these data broker practices.

B. From Social Media Platform to Data Broker: Facebook's Evolution

The face of Big Data is evolving. Though Facebook began as a social networking platform, this section explores the company's evolution into a modern-day data broker.

When Antonio García Martínez, a former Facebook employee who invented the company's targeted ad technology, began working for the company in 2011, there were no in-feed ads on the platform.[89] At that time, a Facebook user visiting the site only saw small "postage-stamp-sized" ads on the right-hand side of the feed.[90] In an interview for the technology and culture podcast Reply All, Martínez explained that he and three engineers discovered how to harness a user's data to deliver them targeted ads.[91] When a Facebook user logged into the website, their device told Facebook their location.[92] This meant that suddenly Facebook knew when a user traveled, just because they logged in from an unfamiliar location.[93]

In 2012, Martínez and his team devised a way to continue tracking Facebook users across the internet (even after they left the website) using a small piece of code called Facebook Pixel.[94] Installed on millions of websites, Facebook Pixel acts as "an internet surveillance camera."[95] It watches everything a person does on a website (like how long someone lingers on a certain webpage, whether someone purchases a product, and if someone adds something to their cart but decides not to buy it) and reports the data back to Facebook.[96]

Once Facebook perfected online tracking, it began purchasing people's offline histories, too.[97] In 2012, Facebook began buying data from

88. *See supra* note 82.
89. *See* Reply All, *supra* note 3, at 03:59.
90. *Id.* at 04:30.
91. *Id.* at 04:28.
92. *Id.* at 04:50.
93. *Id.* at 05:35.
94. *Id.* at 05:50.
95. *Id.* at 06:12.
96. *Id.* at 06:20.
97. *Id.* at 07:30.

Datalogix,[98] a data broker that "collects information from store loyalty cards, [and] says it has information on more than $1 trillion in consumer spending 'across 1400+ leading brands.'"[99] Following its partnership with Datalogix, the company entered into deals with five other data brokers[100] in a program it called "Partner Categories."[101] This program "allowed advertisers to tap into the shadow profiles crafted with data from Facebook and the brokers" to deliver hyper-specific ads for their target audiences.[102] In practice, this meant that "[a] marketer who wanted to target new mothers . . . could use the data brokers' information to send Facebook ads to all women who bought baby formula with a store rewards card."[103] When the ads that the data brokers helped place made a sale, the brokers "got a cut" and Facebook shared information with them about the ad's performance.[104]

While Partner Categories was operational,[105] Facebook combined the brokers' data with its own to create at least 52,000 "unique attributes that [it] . . . used to classify users."[106] These incredibly specific and "mind boggling"[107] categories included "Pretending to Text in Awkward Situations" and "Breastfeeding in Public."[108] At the time, Facebook's website told users that it obtained information about its users "from a few different sources."[109] Jeffrey Chester, the executive director for the Center for Digital Democracy, criticized Facebook's opaque disclosure, calling the move dishonest.[110] Users were not told that those sources included "detailed

98. Julia Angwin et al., *Facebook Is Quietly Buying Information from Data Brokers About Its Users' Offline Lives*, INSIDER (Dec. 30, 2016, 7:56 AM) [hereinafter Angwin et al., *Facebook Is Quietly Buying*], https://www.businessinsider.com/facebook-data-brokers-2016-12.

99. Beckett, *supra* note 33.

100. Angwin et al., *Facebook Is Quietly Buying*, *supra* note 98.

101. Drew Harwell, *Facebook, Longtime Friend of Data Brokers, Becomes Their Stiffest Competition*, WASH. POST (Mar. 29, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/facebook-longtime-friend-of-data-brokers-becomes-their-stiffest-competition/.

102. *Id.*

103. *Id.*

104. *Id.*

105. *See id.* (noting Facebook's end to the program in 2018).

106. *See* Angwin et al., *Facebook Is Quietly Buying*, *supra* note 98; *see also* Julia Angwin et al., *Breaking the Black Box: What Facebook Knows About You*, PROPUBLICA (Sept. 28, 2016), https://www.propublica.org/article/breaking-the-black-box-what-facebook-knows-about-you.

107. Reply All, *supra* note 3, at 09:24.

108. Angwin, et al., *Facebook Is Quietly Buying*, *supra* note 98.

109. *Id.*

110. *Id.*

dossiers obtained from commercial data brokers about users' offline lives," and users were not shown "any of the often remarkably detailed information" Facebook obtained through Partner Categories.[111] Facebook users were not made aware that Facebook was "bundling a dozen different data companies to target" them.[112] When Facebook was asked about its lack of disclosure, it responded that it did not "tell users about the third-party data because it's widely available and was not collected by Facebook."[113]

Facebook continued to work with data brokers in the shadows from 2012 to early 2018, when it announced the end of Partner Categories.[114] Although Facebook claimed that this move would "help improve people's privacy on Facebook," privacy experts viewed the move as "an assertion of dominance" from the technology giant.[115] Facebook's data mining and advertising capabilities had finally eclipsed those of the data brokers that came before it.[116] Facebook no longer needed the data brokers because it had evolved into one itself.

C. Big Tech Companies Are the New Data Brokers

Facebook and Google are now data brokers in every way but name. They even fall squarely under the FTC's definition of "data broker."[117] "When it comes to data, . . . today Acxiom can't hold a candle to Facebook."[118] While Facebook and data brokers "often dealt in the same kinds of personal information advertisers find impossible to resist," Facebook's "first-party data" "served straight from the source, in the person's own words," is more appealing to advertisers than the third-party data that data brokers have aggregated from afar.[119] Instead of using a traditional data broker that claims to capture "more than 80 percent of all U.S. births" from "personal spending and demographic data . . . of women they predict are new and expectant

111. *Id.*
112. *Id.*
113. *Id.*
114. *See* Harwell, *supra* note 101.
115. *Id.*
116. *Id.* (recognizing that Facebook's decision to stop purchasing data from brokers was "a definitive signal that Facebook's data capture and identity-targeting technology is light-years ahead of its competitors").
117. *See generally* FTC, DATA BROKERS, *supra* note 30, at i (defining data brokers as "companies that collect consumers' personal information and resell or share that information with others").
118. Phil Simon, *Facebook: The New King of Data Brokers?*, WIRED, https://www.wired.com/insights/2014/10/facebook-king-data-brokers/ (last visited Jan. 7, 2022).
119. Harwell, *supra* note 101.

mothers," advertisers can tap directly into Facebook's own data trove where people post about life events and freely share photos of their babies.[120] When it comes to online advertising, Facebook's and Google's business models have eliminated the need to buy data from other sources because their data is better.

Facebook and Google use the same core surveillance-based business model, which Amnesty International breaks down into three main parts. First, the companies "develop digital products and services that people find useful and then collect extensive data about people who use or interact with these platforms."[121] These products and services range from Google Maps[122] and Fitbit[123] to Facebook's digital messaging platforms, Messenger and WhatsApp.[124] Importantly, the companies collect data from people who might not even be signed up to use these products and services.[125] Second, they use algorithms to analyze the aggregated data, sort people into categories, and predict people's behavior and interests.[126] Third, the companies "sell access to the information to anyone who wishes to target a defined group of people. The primary aim of the companies' business is to sell advertising placements enabling marketers and advertisers to target people online."[127] While Google and Facebook are two key examples of this business model, other tech giants like Amazon and Microsoft also rely on this model.[128]

Not only does this business model benefit advertisers, who can target specific audiences using these platforms with pinpoint precision, but it has also made the technology companies "the richest companies in the history of humanity."[129] Together, Facebook and Google are responsible for approximately 70% of the world's online ad revenues.[130] In 2021, Facebook's

120. *Id.*

121. SURVEILLANCE GIANTS, *supra* note 15, at 10.

122. David Nield, *All the Ways Google Tracks You—and How to Stop It*, WIRED, https://www.wired.com/story/google-tracks-you-privacy/.

123. SURVEILLANCE GIANTS, *supra* note 15, at 14, 14 n.49 (explaining how Google gained "access to one of the world's largest databases of activity, exercise and sleep data" by acquiring Fitbit).

124. *Id.* at 5.

125. *Id.* at 10.

126. *Id.* at 10.

127. *Id.*

128. *See id.*

129. THE SOCIAL DILEMMA, *supra* note 28, at 16:12.

130. *See Digital Advertising Report 2021*, STATISTA (Dec. 2021), https://www.statista.com/study/42540/digital-advertising-report/ (explaining that worldwide digital ad revenue

revenue from advertising was 97% of its total revenue[131] and Google's was 81.5%.[132] Translated to U.S. dollars, Facebook generated $114.9 billion in 2021 from online advertising alone,[133] and Google brought in $209.5 billion during the same period.[134] Despite the financial benefits this business model brings to Big Tech companies and online advertisers, it comes at an incredible cost to society as a whole. We live in a world where online privacy is a farce, and Big Data knows more intimate details about our lives than our closest friends.

II. The Dangers of Surveillance-Based Business Models

"So what if Google knows a lot about me: I'm still getting a lot for free, right?"[135] To the uninitiated, this might seem like a fair question. But this mindset encapsulates society's fundamental misunderstanding about its relationship to personal data and the tech giants who hoard and manipulate it. All of the "services on the Internet that we think of as free" are really "paid for by advertisers."[136] The platforms' customers are not its users—the advertisers are.[137] They pay companies like Google, Facebook, Twitter, Snap,

---

was $465.5 billion in 2021); S. Dixon, *Meta: Advertising Revenue Worldwide 2009–2021*, STATISTA (Feb. 18, 2022) https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ (illustrating that Facebook's worldwide advertising revenue amounted to $114.93 billion in 2021); Joseph Johnson, *Google: Annual Advertising Revenue 2001–2021*, STATISTA (Feb. 7, 2022), https://www.statista.com/statistics/266249/advertising-revenue-of-google/ (showing that Google's worldwide advertising revenue in 2021 was $209.49 billion). This is an increase from 2019 when these companies accounted "for more than 60% of online ad revenues worldwide." SURVEILLANCE GIANTS, *supra* note 15, at 12.

131. Press Release, Meta, Meta Reports Fourth Quarter and Full Year 2021 Results (Feb. 2, 2022), https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (reporting a total revenue of $117.9 billion).

132. *See* Kim Lyons, *Google Parent Company Alphabet Broke $200 Billion in Annual Revenue for the First Time*, VERGE (Feb. 1, 2022, 4:54 PM EST), https://www.theverge.com/2022/2/1/22912196/google-alphabet-200-billion-annual-revenue-youtube-pixel-search (explaining that Google's total revenue in 2021 was $257 billion); *Google: Annual Advertising Revenue 2001–2021*, *supra* note 130 (reporting that Google's ad revenue was $209.49 billion in 2021).

133. *Meta: Advertising Revenue Worldwide 2009–2021*, *supra* note 130.

134. *Google: Annual Advertising Revenue 2001–2021*, *supra* note 130.

135. David Koff, *Why Google Knows So Much About You: How Their Ecosystem Works & How You Can Defeat It*, MEDIUM (Aug. 19, 2019), https://thetechtutor.medium.com/why-google-knows-so-much-about-you-4aae2ef33832.

136. THE SOCIAL DILEMMA, *supra* note 28, at 14:06.

137. *See id.* at 14:17.

YouTube, and Instagram[138] to display ads to users with "what every business has always dreamt of: to have a guarantee that if it places an ad, it will be successful. . . . They [tech companies] sell certainty."[139] To successfully sell this certainty, the companies must be able to make accurate predictions about their users.[140] And to make great predictions, the companies need "a lot of data."[141]

A. Coerced and Confused: Consumer "Consent"

Before Big Data companies may begin plugging someone's data into their prediction models, they must first obtain consent. Unfortunately for users, "platforms have a grotesque interpretation of consumer consent."[142]

When faced with legal terms and service conditions, the vast majority of Americans, including Chief Justice Roberts of the United States Supreme Court,[143] click "I agree" without reading them.[144] By blindly "consenting" to the terms, conditions, and privacy policies of most technology companies, people permit Google to scan all of their emails[145] and authorize Facebook to track their phone calls and text messaging history.[146] When the media calls out companies for such practices, like in 2018 when the *New York Times* published that Facebook gave companies like Amazon, Spotify, Microsoft, and Netflix "far greater access to people's data than it has disclosed,"[147] the

138. *See id.* at 13:36.

139. *Id.* at 15:01.

140. *Id.* at 15:13.

141. *Id.*

142. Hoofnagle, *Facebook and Google*, *supra* note 20.

143. *See* Uri Benoliel & Shmuel I. Becher, *The Duty to Read the Unreadable*, 60 B.C. L. REV. 2255, 2257 (2019).

144. *See* Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, INSIDER (Nov. 15, 2017. 6:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 (citing to a 2017 Deloitte survey of two thousand U.S. consumers that found that "91% of people consent to legal terms and services conditions without reading them. For younger people, ages 18-34 the rate is even higher with 97% agreeing to conditions before reading").

145. *See* Samuel Gibbs, *Gmail Does Scan All Emails, New Google Terms Clarify*, GUARDIAN (Apr. 15, 2014, 8:24 EDT), https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify.

146. *See* SURVEILLANCE GIANTS, *supra* note 15, at 16 (noting that Facebook "tracks users on Android through its apps, including logging people's call and SMS history – although the company stated it only does so with user consent").

147. Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (explaining that "Facebook allowed Microsoft's Bing search

company responded with, "well, users gave permission."[148] And the companies are not wrong. Because of the duty-to-read doctrine in contract law, which says that "a contracting party has a burden to read an agreement before assenting to its terms," consumers enter into a legally binding contract when they click "I agree," regardless of whether they have read the agreement.[149]

This is by design. By requiring people to consent to lengthy terms of use and privacy policies in order to use their services, "Google and Facebook structure the transaction costs to encourage disclosure."[150] Companies like Facebook and Google "can afford to abuse privacy, because people have no choice but to accept."[151] While users technically do permit these companies to access their data, "the scope of access, how permission is asked, the purpose for which data is used, the duration of the permission, and revocation of permission"[152] are generally unclear and often unreadable for the majority of the population.[153] Two law professors conducted a study in 2019 that "found that 99% of the 500 most popular U.S. websites had terms of service written as complexly as academic journals, making them inaccessible to most people."[154] Also in 2019, *New York Times* journalist Kevin Litman-Navarro read and analyzed the length and readability of privacy policies for 150 popular websites and apps.[155] Not only did he find that the "vast majority" of privacy policies exceeded a college reading level, but he also discovered that Google's 2018 privacy policy was a thirty-minute read.[156]

---

engine to see the names of virtually all Facebook users' friends without consent . . . and gave Netflix and Spotify the ability to read Facebook users' private messages").

148. Hoofnagle, *Facebook and Google*, *supra* note 20; *see also* Elizabeth Schulze, *Facebook Let Tons of Companies Get Info About You, Including Amazon, Netflix, and Microsoft*, CNBC (Dec. 19, 2018, 5:01 PM EST), https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html.

149. *See* Benoliel & Becher, *supra* note 143, at 2257, 2264.

150. Hoofnagle, *Facebook and Google*, *supra* note 20.

151. SURVEILLANCE GIANTS, *supra* note 15, at 41.

152. Hoofnagle, *Facebook and Google*, *supra* note 20.

153. *See* Benoliel & Becher, *supra* note 143, at 2279–80. For more on how new legislation is addressing these problems, see Part III.

154. Jessica Guynn, *What You Need to Know Before Clicking 'I Agree' on That Terms of Service Agreement or Privacy Policy*, USA TODAY (Jan. 29, 2020, 2:21 PM ET), https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/.

155. Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. TIMES, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (last visited Aug. 29, 2021).

156. *Id.*

Even the small percentage of people who do read privacy policies and terms of service agreements when signing up for a service are at risk of opting into harmful data practices disguised as improvements down the road. Platforms strategically "impose so many decision opportunities that privacy management is literally impossible."[157] In 2016, for example, Google "quietly erased" lines in its privacy policy, eliminating its ban on personally identifiable web tracking.[158] This change marked a drastic departure from the company's nearly decade-long practice of keeping users' names separate from its anonymous online ad tracking.[159] In a statement about Google's privacy policy change, Google spokeswoman Andrea Faville wrote that "the change 'is 100% optional—if users do not opt-in to these changes, their Google experience will remain unchanged.'"[160] Instead of being forthright about this change, Google tricked users into opting-in "through a request with titles such as 'Some new features for your Google account.'"[161] Once these companies have obtained your "consent," there is nothing stopping them from using your information in essentially any way they wish.

B. The Manipulation-Based Business Model

As advertisers are increasingly willing to pay technology companies top dollar to target hyper-specific groups of users, the companies are incentivized to addict users to their platforms. According to former Big Tech employees and leading technology industry experts,[162] it is "too simplistic" to say that our data is what is being sold.[163] Instead, our attention is the product.[164] Using aggregated user data and constant surveillance across the internet, technology

157. Hoofnagle, *Facebook and Google*, *supra* note 20.

158. Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*, PROPUBLICA (Oct. 21, 2016, 8:00 AM EDT), https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.

159. *See id.*

160. *Id.*

161. *Id.*

162. In August 2020, Netflix released a documentary entitled "The Social Dilemma," which explores the impact that social networking technology has on human psychology and society. The documentary features internationally renowned experts on the technologies and business models underlying social media companies' most successful features, including former employees, academics, and other researchers. *See* THE SOCIAL DILEMMA, *supra* note 28.

163. *See id.* at 14:20.

164. *See id.* at 14:18.

companies "build models that predict our actions"[165] and are designed to keep users engaged for as long as possible.[166]

Many technology companies have three main goals: (1) "the engagement goal: to drive up your usage, to keep you scrolling"; (2) "the growth goal: to keep you coming back and inviting . . . friends and getting them to invite more friends"; and (3) "the advertising goal: to make sure that, as all that's happening, [they are] making as much money as possible from advertising."[167] To maximize engagement, growth, and advertising, companies use powerful algorithms to determine what content to show users.[168]

The algorithms are written by humans but have minds of their own.[169] Through a process known as "machine learning," programmers give a computer a "goal state," or a desired outcome, and the computer itself learns how to deliver the result.[170] Every day, the computer "gets slightly better at picking the right posts in the right order so that you spend longer and longer" on the platform.[171] And while human programmers control the inputs, "no one really understands what [the computers are] doing in order to achieve that goal."[172]

Because these algorithms control what we see and because they have "almost no human supervision,"[173] "they're controlling us more than we're controlling them."[174] In optimizing their business models to achieve the aforementioned goals, social media and technology companies have created "'persuasion architectures' that can manipulate and influence people at the scale of billions."[175]

---

165. *Id.* at 17:50.

166. *Id.* at 13:35; *see also* Nathalie Maréchal & Ellery Roberts Biddle, *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge*, NEW AM. 1, 5 (Mar. 17, 2020), https://d1y8sb8igg2f8e.cloudfront.net/documents/REAL_FINAL-Its_Not_Just_the_Content_Its_the_Business_Model.pdf (noting that the "ultimate purpose" of content algorithms is "to generate profits for companies by keeping users engaged").

167. THE SOCIAL DILEMMA, *supra* note 28, at 18:50.

168. *Id.* at 19:20.

169. *See id.* at 48:30.

170. *Id.* at 48:00.

171. *Id.* at 48:13.

172. *Id.* at 48:19.

173. *See id.* at 17:24.

174. *Id.* at 48:48.

175. SURVEILLANCE GIANTS, *supra* note 15, at 30 (noting the persuasive nature of algorithms in "find[ing] the best ways to nudge people towards particular outcomes").

1. Content-Shaping Algorithms Create Echo Chambers

The algorithms that control what information individuals see online are known as "content-shaping algorithms."[176] The most visible examples of such algorithms include Facebook's News Feed, YouTube's recommendation engine,[177] and TikTok's For You Page. Companies market these algorithms as ways to show users the content most relevant to them.[178] People believe these recommendation and personalization features are designed to serve them precisely the content they want, but this is simply not the case.[179] Instead, "relevance is measured by predicted engagement: how likely users are to click, comment on, or share a piece of content."[180] The more accurately a company can predict the types of content a user is likely to engage with, the more valuable that company is to advertisers. This incentivizes companies to create individualized echo chambers that "filter[] the information people receive so that it largely supports their existing opinions."[181]

When someone types "Climate change is" in the Google search bar, for example, the suggested autocompletions vary from person to person.[182] Some people will see "climate change is a hoax," but others will see "climate change is causing the destruction of nature."[183] This is "a function not of what the truth is about climate change, but about where you happen to be Googling from and the particular things that Google knows about your interests."[184]

When individuals only consume information designed to cater to their worldviews, people begin "operating on a different set of facts."[185] At scale, people are rendered unable "to reckon with or even consume information that contradicts" that specially curated worldview.[186] According to Rashida Richardson, a professor at NYU School of Law, "That means we aren't actually being objective, constructive individuals."[187]

176. Maréchal & Biddle, *supra* note 166, at 13.
177. *Id.*
178. *See id.*
179. *See* THE SOCIAL DILEMMA, *supra* note 28, at 59:37.
180. Maréchal & Biddle, *supra* note 166, at 14.
181. Roheeni Saxena, *The Social Media "Echo Chamber" Is Real*, ARS TECHNICA (Mar. 13, 2017, 1:25 PM), https://arstechnica.com/science/2017/03/the-social-media-echo-chamber-is-real/.
182. THE SOCIAL DILEMMA, *supra* note 28, at 55:22.
183. *Id.*
184. *Id.*
185. *Id.* at 57:11.
186. *Id.*
187. *Id.*

This echo chamber phenomenon on social media becomes particularly concerning when it comes to news consumption. In 2016, a survey by Pew Research Center found that 62% of adults consume their news on social media.[188] News consumption on Facebook is "dominated by selective exposure, meaning that people are most often exposed to news sources that reinforce their existing opinions."[189] This is a key reason why so much of online discourse devolves into a showdown between "us versus them."[190] Experts warn that these algorithms are actually "increasing polarization in society."[191] And technology companies thrive on this polarization because it is "extremely efficient at keeping people online."[192]

While for years Facebook CEO Mark Zuckerberg denied that the company designed its products to maximize user engagement, former Facebook employee-turned-whistleblower Frances Haugen exposed the truth when she disclosed a trove of internal Facebook documents, known as the "Facebook Papers," to the U.S. Securities and Exchange Commission in October 2021.[193] Among the most shocking revelations was that, from 2017 to 2020, Facebook's algorithm gave five times more weight to "angry" emoji reactions than "likes," boosting divisive and provocative content in users' feeds.[194] Data scientists at Facebook confirmed that posts prompting "angry" reactions "were disproportionately likely to include misinformation" and toxic content.[195] And when the company set the "angry" reaction's weight to zero in September 2020, the algorithm exposed users to less misinformation and "disturbing" content.[196]

---

188. Jeffrey Gottfried & Elisa Shearer, *News Use Across Social Media Platforms 2016*, PEW RSCH. CTR. (May 26, 2016), https://www.pewresearch.org/journalism/2016/05/26/news-use-across-social-media-platforms-2016/.

189. Saxena, *supra* note 181.

190. *See* Giovanni Luca Ciampaglia & Filippo Menczer, *Biases Make People Vulnerable to Misinformation Spread by Social Media*, SCI. AM. (June 21, 2018), https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/.

191. *See, e.g.*, THE SOCIAL DILEMMA, *supra* note 28, at 58:40 (referencing the algorithm behind YouTube's recommendation system).

192. *Id.* at 58:50.

193. *See* Cristiano Lima, *A Whistleblower's Power: Key Takeaways from the Facebook Papers*, WASH. POST (Oct. 26, 2021, 7:00 AM EDT), https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/.

194. *Id.*

195. Jeremy B. Merrill & Will Oremus, *Five Points for Anger, One for a 'Like': How Facebook's Formula Fostered Rage and Misinformation*, WASH. POST (Oct. 26, 2021), https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/.

196. *Id.*

2. Echo Chambers Amplify Conspiracy Theories and Divisive Content

When platforms selectively expose users to information that reinforces their opinions, and when recommendation engines are designed to send people down rabbit holes,[197] radical ideas once confined to the fringes of the internet can find their way into the mainstream. A timely example of this is the explosion of QAnon in the United States. QAnon is an elaborate, disproven, "big tent" conspiracy theory[198] whose supporters believe that former President Trump is "fighting a global child-trafficking network led by satanic, cannibalistic left-wing pedophile elites."[199] QAnon was born in October 2017 when an anonymous account now known as "Q" posted on 4chan, a "notoriously toxic message board."[200] The anonymous poster "claimed to be a high-ranking government insider with access to classified information" about Trump's war on the global pedophile cabal.[201] The theory's supporters initially existed only on the fringes of the internet, but over time started making their way onto more mainstream platforms like Twitter, YouTube, and Facebook.[202] As they migrated, the posts, memes, and videos they used to explain their ideology "became more accessible and digestible."[203] And as the group's messaging appealed more to the masses, QAnon exploded in popularity.

The extremist ideology, paired with Facebook's recommendation algorithm, which suggests various groups users might be interested in joining, created a "dangerous combination."[204] The FBI categorized QAnon as a "potential domestic terror threat" in 2019 when its supporters began committing violent crimes, including kidnapping, assault, and attempted murder, in the real world.[205]

In March 2020, when millions of Americans were confined to their homes due to the COVID-19 pandemic and were spending a lot of time online,

197. *See* THE SOCIAL DILEMMA, *supra* note 28, at 58:40 (explaining how the YouTube recommendation algorithm works).

198. Vox, *The Instagram Aesthetic That Made QAnon Mainstream*, YOUTUBE, at 2:14 (Oct. 28, 2020) [hereinafter *The Instagram Aesthetic That Made QAnon Mainstream*], https://www.youtube.com/watch?v=_7FWr2Nvf9I.

199. *Id.* at 1:33.

200. Kevin Roose, *What Is QAnon, the Viral Pro-Trump Conspiracy Theory?*, N.Y. TIMES (Sept. 3, 2021), https://www.nytimes.com/article/what-is-qanon.html.

201. *Id.*

202. *See, e.g.*, *The Instagram Aesthetic That Made QAnon Mainstream*, *supra* note 198, at 1:45.

203. *Id.*

204. *Id.* at 2:18.

205. *Id.* at 2:57.

"three leading QAnon Facebook groups saw their membership rise from under 50,000 to over 300,000."[206] By August, Facebook found that QAnon groups and pages on its platform had more than three million followers.[207] On August 19, when Facebook announced that it had banned QAnon content and shut down hundreds of related groups and pages,[208] the group rebranded, co-opting the hashtag "Save The Children" from a legitimate anti-trafficking group's hashtag campaign.[209]

At the same time, the QAnon base moved to Instagram, a Facebook-owned platform. While accounts that already had high followings on the platform began promoting the hashtag, so too did smaller accounts, which used "#savethechildren" as "an Internet cheat code."[210] Accounts that usually received only a few hundred likes per post "found themselves getting tens of thousands of likes as soon as they started posting about 'Save the Children.'"[211] This engagement fueled QAnon's growth on the platform and continued the group's promotion of false and harmful information.

QAnon's rebranding and surge in popularity led to two major, real-world consequences. First, the Save the Children movement spread inaccurate information that made it more difficult for legitimate organizations to fight actual trafficking.[212] QAnon's supporters "made it harder for people with real information about possible human trafficking victims to get through."[213] Second, in 2020, more than twenty QAnon-supporting candidates ran for U.S. Congress.[214] Although the belief in QAnon theories falls on a spectrum, and most people who attended Save the Children rallies do not believe that Hillary Clinton actually "eats children," the extremist ideology is designed to send people down rabbit holes, "radicaliz[ing] them according to their own personality type."[215] The hysteria that compounds as people crawl deeper down those rabbit holes "could more than likely eventually lead to [their] thinking that Hillary Clinton eats children."[216] The danger is that "people

206. *Id.* at 3:10.

207. *Id.* at 3:37.

208. Jack Brewster, *QAnon Traffic Declined After Facebook Cracked Down*, FORBES (Sept. 10, 2020, 3:07 PM EDT), https://www.forbes.com/sites/jackbrewster/2020/09/10/qanon-traffic-declined-after-facebook-cracked-down/?sh=1d359d534fb0.

209. *Id.*; *see also* Roose, *supra* note 200.

210. *The Instagram Aesthetic That Made QAnon Mainstream*, *supra* note 198, at 5:26.

211. *Id.* at 5:40.

212. *See id.* at 6:12.

213. *Id.* at 7:47.

214. *Id.* at 9:01.

215. *Id.* at 8:32.

216. *Id.*

don't need to believe, or even be aware of, the entirety of a conspiracy theory for it to start influencing their decisions."[217] And in the 2020 election, this influence led to two of the twenty QAnon supporters actually winning seats in Congress.[218]

This is only one of the most recent examples of how social media platforms' persuasion architectures have been exploited to manipulate society and impact its political processes. Russia's interference in the 2016 U.S. presidential election is another example.[219] In this case, the Russians did not hack or hijack Facebook. Instead, "they used the tools that Facebook created for legitimate advertisers and legitimate users, and they applied it to a nefarious purpose."[220] When influence and persuasion capabilities are deployed on a large scale on platforms like Facebook, Instagram, and YouTube, companies have the power to influence peoples' opinions, but other actors do too.[221]

3. Divisive Content Erodes Democracy

On January 6, 2021, Nick Alvear, an activist filmmaker, cheered from the top steps outside the U.S. Capitol, his camera trained on the mob of fellow Trump supporters plowing their way inside the building.[222] Alvear was one of an estimated 2,500 people who breached the Capitol on January 6 to protest the outcome of the 2020 presidential election and disrupt Congress's certification of President Joe Biden's election win.[223] What drew him to Trump? Save the Children.[224] In an interview for an HBO documentary about the January 6 insurrection, Alvear explains, "I believed in [Trump's] message. And 800,000 kids go missing a year in the United States . . . . That's usually what gets people into the door supporting Trump . . . we can all relate to having love for children."[225] As the documentary cuts to Alvear's footage of the Capitol's Rotunda teeming with rioters, Alvear explains that he

217. *Id.* at 9:04.

218. Katherine Tully-McManus, *QAnon Goes to Washington: Two Supporters Win Seats in Congress*, ROLL CALL (Nov. 5, 2020, 11:21 AM), https://www.rollcall.com/2020/11/05/qanon-goes-to-washington-two-supporters-win-seats-in-congress/.

219. *See* THE SOCIAL DILEMMA, *supra* note 28, at 1:11:51.

220. *Id.* at 1:12:18.

221. *See* SURVEILLANCE GIANTS, *supra* note 15, at 31.

222. FOUR HOURS AT THE CAPITOL, at 38:37 (HBO 2021).

223. *See* Ryan Lucas, *Where the Jan. 6 Insurrection Investigation Stands, One Year Later*, NPR (Jan. 6, 2022, 5:00 AM ET), https://www.npr.org/2022/01/06/1070736018/jan-6-anniversary-investigation-cases-defendants-justice.

224. *See* FOUR HOURS AT THE CAPITOL, *supra* note 222, at 39:14.

225. *Id.*

believes he is "part of the first wave that is bringing . . . awareness" to the movement.[226]

QAnon was among more than a dozen other extremist groups represented at the Capitol that day, including the Proud Boys, the Oath Keepers, the Three Percenters, the Nationalist Socialist Club (a hate group known to disrupt Black Lives Matter protests), and No White Guilt.[227] Their unifying cause—Stop the Steal.

In the hours after polls closed on November 3, 2020, "angry Donald Trump supporters on Facebook coalesced around a rallying cry now synonymous with the siege on the U.S. Capitol: 'Stop the Steal.'"[228] Trump supporters flooded the social media site with disinformation about election results, "perpetuat[ing] the lie that the election had been stolen from then-President Donald Trump—a lie that Trump himself had been stoking for months."[229] On November 5, Facebook banned the explosively popular "Stop the Steal" Facebook group, which had amassed more than 360,000 members in less than two days and was gaining "tens of thousands" of new members every hour.[230] Justifying the ban on the group and all other groups with similar names, the company "cited the prevalence of posts calling for violence and using hate speech" within those groups.[231] Despite this move, Facebook hardly made a dent in the surge of disinformation and insurrection threats that spread on the social media site between Election Day and the January 6 insurrection.[232] In fact, according to a joint *ProPublica* and *Washington Post* investigation analyzing millions of Facebook posts, leaked internal company documents, and interviews with former employees, Facebook "played a critical role in the spread of false narratives that fomented the violence of Jan. 6."[233]

---

226. *Id.*

227. Masood Farivar, *Researchers: More Than a Dozen Extremist Groups Took Part in Capitol Riots*, VOA (Jan. 16, 2021, 8:47 PM), https://www.voanews.com/a/2020-usa-votes_researchers-more-dozen-extremist-groups-took-part-capitol-riots/6200832.html.

228. Shannon Bond & Bobby Allyn, *How the 'Stop the Steal' Movement Outwitted Facebook Ahead of the Jan. 6 Insurrection*, NPR (Oct. 22, 2021, 9:50 PM ET), https://www.npr.org/2021/10/22/1048543513/facebook-groups-jan-6-insurrection.

229. *Id.*

230. *See id.*

231. Craig Silverman et al., *Facebook Hosted Surge of Misinformation and Insurrection Threats in Months Leading Up to Jan. 6 Attack, Records Show*, PROPUBLICA (Jan. 4, 2022, 8:00 AM EST), https://www.propublica.org/article/facebook-hosted-surge-of-misinformation-and-insurrection-threats-in-months-leading-up-to-jan-6-attack-records-show.

232. *See id.*

233. *Id.*

Facebook began heavily promoting groups as a way to drive user engagement in 2017.[234] In the months leading up to Election Day 2020, Facebook established a special task force to police groups focused on U.S. politics because of how "toxic" they had become.[235] While the task force removed "hundreds of groups with violent or hateful content in the months before Nov. 3," Facebook disbanded the task force and pulled back on other enforcement measures "shortly after the vote."[236] Because of Facebook's decision, in the "nine increasingly tense weeks" leading up to the January 6 insurrection, Facebook groups "were inundated with posts attacking the legitimacy of Biden's election while the pace of removals noticeably slowed."[237] While content removal picked up again the week of January 6, the "lull in enforcement" allowed "hundreds of thousands of posts question[ing] the legitimacy of Biden's victory," "lies about voter fraud," and "call[s] for violence" to run rampant in the interim[238]—arguably when such policing measures mattered most. Facebook was not the only website to host extreme content in the lead-up to the January 6 attack, but Trump "used Facebook as a key platform for his lies about the election right up until he was banned on Jan. 6. And Facebook's reliance on groups to drive engagement gave those lies unequaled reach."[239]

While Facebook cannot be held solely responsible for the proliferation of false information surrounding the 2020 election results that led to an attack on American democracy, *ProPublica* and the *Washington Post*'s analysis reveals that Facebook's failure to effectively police the dissemination of such information played a key role in the harmful narrative's spread. Until new legislation is enacted to curtail similar practices, Facebook and other technology and social media companies will continue to facilitate the radicalization of their users,[240] contribute to real-world harms, and threaten the bedrock of society.

As the discussion above has shown, Big Data's current data practices pose myriad threats—not only to individual American consumers, but also to society at large. This Part continues by introducing the internationally

234. *See id.*
235. *Id.*
236. *Id.*
237. *Id.*
238. *Id.*
239. *Id.*
240. *See* Evelyn Mary Aswad, *Losing the Freedom to Be Human*, 52 COLUM. HUM. RTS. L. REV. 306 (2020) (exploring the impact that digital technologies and contemporary business models have on the human right to freedom of opinion).

recognized human right to privacy and exploring how these companies' practices fall short of the international standards designed to protect this right.

C. The Human Right to Privacy

1. Identifying the Nature of the Right

International human rights law recognizes a fundamental right to privacy that governments are required to follow and U.S. companies are expected to respect in their operations. This section identifies international texts that establish the right to privacy and incorporates work by leading UN privacy experts in attempting to define what the right entails. It also outlines steps that U.S. companies are expected to take in guaranteeing the right to privacy.

Two key texts in international law specifically provide for the human right to privacy. First, the Universal Declaration of Human Rights ("UDHR") provides that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . . . Everyone has the right to the protection of the law against such interference or attacks."[241] Second, the International Covenant on Civil and Political Rights ("ICCPR") provides that "[n]o one shall be subjected to *arbitrary or unlawful* interference with his privacy, family, home or correspondence . . . . Everyone has the right to the protection of the law against such interference or attacks."[242] While the UDHR is merely an aspirational document that proclaimed a "standard of achievement for all peoples and all nations" to follow in the wake of World War II,[243] the ICCPR is a legally binding treaty to which the U.S. government is a party.[244] Thus, it has the same status as federal law.[245] While treaties are normally only binding on state actors, the U.S. government has made clear

241. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948) [hereinafter UDHR].

242. International Covenant on Civil and Political Rights, art. 17, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) (emphasis added).

243. *See* UDHR, *supra* note 241, at pmbl.

244. *4. International Covenant on Civil and Political Rights*, UN TREATY COLLECTION, https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV4&src=IND (last visited Jan. 7, 2022).

245. *See* U.S. CONST. art. VI, § 2. While the ICCPR is part of U.S. law, it is technically a "non-self-executing" treaty. *See* BARRY E. CARTER, ET AL., INTERNATIONAL LAW 191 (7th ed. 2018). Accordingly, Congress must have passed implementing legislation for the ICCPR to be enforceable in U.S. courts. *See id.* While Congress has not yet passed implementing legislation for the ICCPR, its status in the hierarchy of U.S. law remains equal to that of federal law, and the U.S. must comply with its international obligations regarding the right to privacy regardless of the treaty's enforceability in domestic courts. *See id.* at 191–92.

its expectation that U.S. companies respect international human rights in their operations.[246]

In recent years, leading experts have set out to clarify the scope of the right to privacy with greater detail. In particular, Joseph Cannataci, the former UN Special Rapporteur on the right to privacy, has advanced his understanding of what the right entails in today's digital landscape.[247] In a 2016 report surveying global perspectives on the right to privacy, Cannataci recognized that the right exists within the context of a "fundamental right to dignity and the free, unhindered development of one's personality."[248] He has similarly noted that "in general, the protection of private life includes other rights and specific guarantees for the storage of information, access to personal data, as well as the regulation on protection of private communications, names, physical and moral integrity."[249] Importantly, in discussing the right in light of new privacy laws that went into effect around the world from 2017 to 2018 (including the European Union's General Data Protection Regulation, which is discussed in more detail below), Cannataci specifically concluded that "the unrestricted sharing of data . . . [is] contrary to the protection of the right to privacy and must cease."[250]

Although these findings do not precisely define the scope of the right to privacy, they do recognize its importance in the digital age. They also suggest that companies are acting inconsistently with international human rights standards by engaging in the unrestricted sharing of users' personal data. As a result, to stop contributing to infringements of their users' human rights, U.S. businesses must stop sharing consumer data in the ways they have grown accustomed.

---

246. *See* U.S. DEP'T OF STATE, BUREAU OF DEMOCRACY, HUM. RTS., & LAB., U.S. GOVERNMENT APPROACH ON BUSINESS AND HUMAN RIGHTS 3–4 (2013); *see also* RESPONSIBLE BUSINESS CONDUCT: FIRST NATIONAL ACTION PLAN FOR THE UNITED STATES OF AMERICA (2016) (outlining a commitment to promoting responsible business conduct by U.S. companies operating abroad, including standards set forth in the UN Guiding Principles on Business and Human Rights).

247. *See Biography of Joe Cannataci, Former Special Rapporteur on the Right to Privacy*, UN OFF. HIGH COMM'R FOR HUM. RTS., https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/JoeCannataci.aspx (last visited Jan. 7, 2022).

248. Joseph Cannataci (Special Rapporteur on the Right to Privacy), *Rep. of the Special Rapporteur on the Right to Privacy*, ¶ 25, U.N. Doc. A/HRC/31/64 (Nov. 24, 2016).

249. Joseph Cannataci (Special Rapporteur on the Right to Privacy), *Right to Privacy*, ¶ 40, U.N. Doc. A/71/368 (Aug. 30, 2016).

250. Joseph Cannataci (Special Rapporteur on the Right to Privacy), *Right to Privacy*, ¶ 109, U.N. Doc. A/73/438 (Oct. 17, 2018).

2. Standards for U.S. Businesses

The United Nations Guiding Principles on Business and Human Rights ("UNGPs"), which the Human Rights Council unanimously endorsed in 2011,[251] established a framework that businesses should follow to promote human rights in their operations.[252] The UNGPs recognize that countries have an obligation to protect human rights and that there are two primary ways for corporations to respect human rights in their operations.[253] First, businesses should respect human rights by avoiding infringing on them.[254] Second, businesses should address the adverse human rights impacts that their operations cause or contribute to.[255] Because the U.S. government has endorsed the UNGPs and stated that it expects U.S. companies to follow them, U.S.-based data and technology companies are expected to respect human rights and provide remedies when their operations cause or contribute to infringements.[256]

The responsibility to respect human rights begins with taking efforts to avoid infringing on those rights recognized in the UDHR and ICCPR and addressing a company's involvement in undermining human rights.[257] This responsibility applies to corporations of all sizes and across all sectors and includes adopting policy commitments, conducting human rights due diligence, and implementing remedy processes.[258] Due diligence should be ongoing and include adverse impacts linked to operations, products, services, and business relationships—even where the company's own activities do not cause adverse impacts.[259] After conducting due diligence, companies should integrate the findings into their operations and track their effectiveness based on both quantitative and qualitative factors, as well as feedback from internal and external sources.[260]

Though businesses are required to respect human rights in their operations, they must also comply with the domestic laws of the countries where they

251. *See* Human Rights Council Res. 17/4, U.N. Doc. A/HRC/RES/17/4, at 2 (July 6, 2011).

252. Guiding Principles on Business and Human Rights, at 1, U.N. Doc. HR/PUB/11/04 (2011) [hereinafter UNGPs].

253. *See id.* at 1.

254. *Id.* at 13.

255. *Id.*

256. *See supra* note 246.

257. *See* UNGPs, *supra* note 252, at 13.

258. *Id.* at 15–16.

259. *Id.* at 17–18.

260. *Id.* at 20–22.

operate.[261] When the obligation to comply with local laws conflicts with the responsibility to respect human rights, companies should treat human rights as a compliance issue and find ways to best protect them.[262] In circumstances where preventing adverse human rights impacts is not possible, corporations should provide remedies to affected persons. In providing access to effective remedies, companies should make these processes legitimate, accessible, predictable, equitable, transparent, and rights-compatible.[263] Together, these principles establish the standards against which the operations of companies like Facebook and Google should be compared.

3. Current Business Practices Fail to Uphold These Standards

It is immediately apparent that these companies are falling well below the standards established by the UNGPs. At a minimum, to respect the human right to privacy, they should be conducting due diligence into how their operations undermine their users' privacy rights and incorporating those findings into their operations. However, industry practice makes clear that companies like Facebook and Google are either choosing not to conduct this due diligence or refusing to incorporate the findings. Rather than taking steps to limit potential infringements on their users' privacy rights, these companies and their counterparts are instead electing to prioritize their own profits.

Beyond merely failing to prevent or limit adverse human rights impacts, data and technology companies are also failing to comply with the second key requirement under the UNGPs: to implement meaningful remedial processes. Rather than compensating users when their personal data is shared with advertisers and other third parties, these companies are turning their backs on the very consumers who make them so profitable. The impunity with which data and technology companies share user data across the internet spotlights their failure to implement accessible, predictable, equitable, and transparent remedies. By both failing to protect users' data in the first place and by further depriving them of remedies after the fact, these companies are infringing on their users' human rights in every way that the UNGPs were designed to prevent. Because these companies have failed to adhere to the best practices established by the UN and championed by the U.S. government, regulation will be a vitally important tool in protecting the privacy rights of consumers.

261. *Id.* at 25.
262. *Id.*
263. *Id.* at 33–34.

III. The Current State of Data Privacy Legislation

In light of the risks that these companies' business models and operations pose for the right to privacy, various countries and U.S. states have begun regulating the collection and use of consumers' personal data. Part III highlights one regional data privacy regulation, five U.S. federal legislative proposals, and several comprehensive state laws and proposals that help showcase both the evolution and current state of data privacy regulation.

A. The European Union's General Data Protection Regulation

The European Union ("EU") took the first major step towards regulating data privacy in 2016 when it adopted the European Union General Data Protection Regulation ("GDPR"). The GDPR was designed to regulate the processing of personal data.[264] In the EU, "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right."[265] The GDPR created much stronger rules for data protection, which gave people "more control over their personal data."[266] The GDPR protects individuals who are physically present in the EU, regardless of citizenship and length of stay.[267] This means that the GDPR applies to EU citizens, tourists, expatriates, cross-border commuters, refugees, and stateless persons, but it does not apply to EU citizens who are physically located outside of the EU.[268]

Since the GDPR entered into force on May 25, 2018, all companies operating in the EU have been subjected to one set of data protection rules, regardless of their geographic bases.[269] This means that, once the law went into effect, companies around the world, including Google, Facebook, and Amazon, became subject to its regulatory framework. Under the GDPR, obligations and duties under the law apply to both "data 'controllers' and data 'processors,' irrespective of size and whether activity is for profit or not."[270]

---

264. 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, 1 (EU), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [hereinafter GDPR].

265. *Id.* at 1.

266. *See EU Data Protection Rules*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en (last visited Jan. 7, 2022).

267. Matthias Artzt, *Territorial Scope of the GDPR from a US Perspective*, IAPP (June 26, 2018), https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/.

268. *Id.*

269. *See EU Data Protection Rules*, *supra* note 266.

270. WIREWHEEL, INC., GDPR VS CCPA: HOW THE DIFFERENCE IMPACTS YOUR DATA PRIVACY OPERATIONS 2 (2020) [hereinafter GDPR VS CCPA].

The GDPR distinguishes data "controllers" from data "processors" because "not all organisations involved in the processing of personal data have the same degree of responsibility."[271] While Article 4(7) of the GDPR defines a "controller" as "the natural or legal person, public authority, agency or other body which, along or jointly with others, determines the purposes and means of the processing of personal data,"[272] Article 4(8) defines a "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[273] Because controllers decide how personal data is used and processed, most of the GDPR's obligations fall on them; meanwhile, processors' compliance responsibilities are more limited.[274]

While the GDPR contains forty-five specific regulations for data collection and processing practices,[275] controllers should, at a minimum, take the six basic but most important steps listed below to comply with the law.[276] First, controllers must obtain consent from data subjects to process their data.[277] This consent must be communicated through clear terms, freely given by the user, and revocable at any time.[278] In practice, businesses are required to "prompt consumers to 'accept' cookies and other tracking technologies before progressing on a website."[279] Importantly, for "consent to be valid . . . , a consumer must *actively confirm* their consent, such as by ticking an unchecked opt-in box."[280] Second, controllers must report security breaches to customers and a supervisory authority within seventy-two hours of becoming aware of a breach.[281] Third, if data subjects request their data profile from a controller, the controller must provide them with a free copy

271. *What Are 'Controllers' and 'Processors'?*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/ (last visited Feb. 16, 2021).

272. GDPR, *supra* note 264, at 33.

273. *Id.*

274. *See* ROBBIE DOWNING, OVERVIEW OF EU GENERAL DATA PROTECTION REGULATION (2020) (Westlaw, Practical Law: Overview W-007-9580).

275. *See* Roslyn Layton & Julian Mclendon, *The GDPR: What It Really Does and How the U.S. Can Charter a Better Course*, 19 FEDERALIST SOC'Y. REV. 234, 234 (2018).

276. *See generally* Sam Saltis, *GDPR Explained in 5 Minutes: Everything You Need to Know*, CORE DNA (Dec. 7, 2020), https://www.coredna.com/blogs/general-data-protection-regulation#2.

277. *See* GDPR, *supra* note 264, at 7.

278. *See id.* at 8.

279. GDPR VS CCPA, *supra* note 270, at 3.

280. *Id.*

281. *See* GDPR, *supra* note 264, at 52–53.

of all of the data about them and explain how that data is being used.[282] Fourth, because the GDPR gives data subjects the "right to be forgotten," controllers must be prepared to remove data in response to valid requests.[283] Pursuant to the right to be forgotten, individuals have the right to request that their data be deleted after it has been used for its original purpose.[284] Fifth, controllers are encouraged to package data "in a structured, commonly used, machine-readable and interoperable format" that enables data portability between controllers.[285] Finally, data controllers should build their systems to include "[p]rivacy by design," which might include measures to minimize the amount of personal data being processed, process personal data in a way that prevents it from being attributed to a particular individual, or allow data subjects to monitor the processing of their data.[286]

The structure of the European Union complicates enforcement of the GDPR. Each EU Member State has one Data Protection Authority ("DPA").[287] DPAs are "independent public authorities" that handle complaints of GDPR violations and have the power to investigate and fine companies to ensure compliance with the law.[288] Ideally, complaints would be distributed evenly across the twenty-eight DPAs, but because of a "quirk" in European law that "funnels complaints to the country where companies have their European headquarters," a substantial amount of the early responsibility for exercising oversight fell "to just one small, underfunded agency, the Irish Data Protection Commission."[289] While other countries' DPAs have begun enforcing the GDPR over the last few years, the disjointed nature of the GDPR's enforcement regime highlights the need for a more

282. *See id.* at 11–12.

283. *See id.* at 12; *see also* Ben Wolford, *Everything You Need to Know About the "Right to Be Forgotten,"* GDPR.EU, https://gdpr.eu/right-to-be-forgotten/ (last visited Jan. 8, 2022).

284. *See* GDPR, *supra* note 264, at 12.

285. *Id.* at 13; *see* Saltis, *supra* note 276.

286. Saltis, *supra* note 276; *see* GDPR, *supra* note 264, at 78 ("[T]he controller should adopt internal policies and implement measures which meet . . . the principles of data protection by design and data protection by default.").

287. *What Are Data Protection Authorities (DPAs)?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en (last visited Jan. 8, 2022).

288. *See id.*

289. Katie Collins, *As the GDPR Turns 2, Big Tech Should Watch Out for Big Sanctions*, CNET (May 24, 2020, 5:00 AM PT), https://www.cnet.com/news/as-the-gdpr-turns-2-big-tech-should-watch-out-for-big-sanctions/.

centralized enforcement system, which is something that Senator Gillibrand provides for in her 2020 and 2021 proposals.[290]

As the first widespread data privacy law in the world, the GDPR has been the subject of significant criticism. One leading critique is that fines under the GDPR are missing the targets: big technology companies.[291] While the tech giants can withstand significant fines, including those totaling many millions of dollars, smaller technology companies often cannot.[292] Instead of using fines to deter the companies that are doing the most damage in terms of online data privacy, the GDPR has the potential to further strengthen the largest technology companies' existing monopolies by wiping out their competition.[293] Between May 2018 and July 2022, approximately 1,270 fines have been levied by DPAs in EU member states.[294] Of those fines, only a small number have been levied against large technology companies based in Silicon Valley. While the DPAs in Luxembourg, Ireland, France, and Spain have levied fines of 10 million euros or more against these companies, including a 746 million euro fine against Amazon's European division in July 2021 and 225 million euro fine against WhatsApp Ireland in September 2021, more than 85% of the fines have been for 100,000 euros or less.[295] And even when data companies receive fines that seem significant, they are much less impressive when placed in context. For example, the Amazon fine represents less than one day's worth of revenue,[296] and a 50 million euro fine levied against Google in 2019[297] amounted to only one-tenth of the company's daily sales.[298] As these figures make clear, the biggest companies can afford to

290. *See infra* Section III.B.1.

291. *See* Alex Moazed, *How GDPR Is Helping Big Tech and Hurting the Competition*, APPLICO, https://www.applicoinc.com/blog/how-gdpr-is-helping-big-tech-and-hurting-the-competition/ (last visited Jan. 8, 2022).

292. *See id.*

293. *See id.*

294. *See GDPR Enforcement Tracker*, CMS.LAW, https://www.enforcementtracker.com/ (last visited July 15, 2022).

295. *See GDPR Enforcement Tracker Report: Executive Summary*, CMS.LAW, https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/executive-summary. *See also id.* (highlighting the disparity in GDPR fine amounts and how the majority of fines have been levied against government entities, smaller businesses, and, in some cases, individuals).

296. *See* Meaghan Yuen, *Amazon Annual Revenue Breakdown by Segment in 2022*, INSIDER INTEL. (Feb. 11, 2022), https://www.insiderintelligence.com/insights/amazon-revenue (forecasting $729.76 billion for Amazon's online sales worldwide in 2022).

297. *See* Collins, *supra* note 289.

298. Adam Satariano, *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, N.Y. TIMES (Apr. 27, 2020), https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html.

continue violating the GDPR while smaller entities and individuals bear the brunt of enforcement.

Large companies that can afford "small armies of lawyers" are no match to the underfunded agencies responsible for GDPR enforcement.[299] Before the GDPR went into effect, several tech giants had already prepared their defenses. Google, for example, spent "hundreds of years of human time and, ostensibly, billions of dollars to shore up its defenses."[300] Just after the GDPR's launch, Facebook reinterpreted the rules for reporting breaches and took two months "instead of the required 72 hours to report a breach affecting 7 million users' private photos."[301] While "the richest companies in the history of humanity"[302] can afford to insulate themselves against the GDPR, smaller companies cannot because they have neither "the time, money, [nor] personnel to tackle privacy compliance."[303] The effect on small and mid-sized companies has already been seen in action. As advertisers choose "to spend more with the platform giants because of their ability to withstand regulatory assaults," European ad-tech companies go extinct.[304] Despite its drawbacks, the GDPR set the stage for data privacy and protection reform around the globe.

B. Recently Proposed Federal Data Privacy Legislation

The United States seriously lags behind Europe in terms of data privacy because it lacks a comprehensive federal data privacy law.[305] Today, there exists only a patchwork of sector-specific federal laws that regulate online privacy and data collection.[306] The main federal mechanism for enforcing

299. Collins, *supra* note 289.

300. Moazed, *supra* note 291 (internal quotation marks omitted).

301. *Id.*

302. THE SOCIAL DILEMMA, *supra* note 28, at 16:08.

303. Moazed, *supra* note 291.

304. *Id.* (emphasis omitted).

305. *See* Samer Kamal, *Where Does the U.S. Rank in the Global Data Privacy Landscape?*, CPO MAG. (Apr. 24, 2020), https://www.cpomagazine.com/data-privacy/where-does-the-u-s-rank-in-the-global-data-privacy-landscape/.

306. *See* Privacy Act of 1974, 5 U.S.C. § 552a (governing collection, maintenance, use, and dissemination of information about individuals maintained in federal records systems); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (requiring financial institutions to explain to consumers how their information is shared); Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (regulating information collection by consumer reporting agencies); Children's Online Privacy Protection Act of 1998, 15 U.S.C §§ 6501–6505 (imposing requirements for online platforms and services directed to children under the age of thirteen); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (regulating the collection of health information).

privacy promises made by companies is 15 U.S.C. § 45, which gives the FTC the responsibility to prevent "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[307] With scarce resources, the FTC is left to prevent only the most pressing threats to online privacy.[308]

1. Senator Gillibrand's Data Protection Act

Following the EU's adoption of the GDPR, American legislators began proposing their own ideas for what data privacy reform could look like in the United States. In February 2020, Senator Kirsten Gillibrand (D-NY) introduced the Data Protection Act of 2020.[309] The proposed legislation would have established the Data Protection Agency ("DPA"), an independent federal agency "that would serve as a 'referee' to define, arbitrate, and enforce rules to defend the protection" of people's personal data.[310] The agency would have been authorized "to (1) enforce federal privacy law, and (2) take specified actions to prevent a covered entity from committing or engaging in an unfair or deceptive act or practice."[311]

Senator Gillibrand explained that the DPA would serve three core missions.[312] First, it would enforce data protection rules, giving Americans control over their own data.[313] The DPA would be authorized by Congress (or itself) to enforce privacy laws around data protection and would enforce such laws through "civil penalties, injunctive relief, and equitable remedies."[314] Additionally, much like the GDPR's Data Protection Authorities, Senator Gillibrand's DPA would "take complaints, conduct investigations, and inform the public on data protection matters."[315]

Second, the DPA would "[w]ork to maintain the most innovative, successful tech sector in the world and ensure fair competition within the

307. 15 U.S.C. § 45(a)(1).

308. *See* Layton & Mclendon, *supra* note 275, at 236.

309. *S.3300 – Data Protection Act of 2020*, CONGRESS.GOV, https://www.congress.gov/bill/116th-congress/senate-bill/3300 (last visited June 13, 2022) [hereinafter *S.3300 – Data Protection Act of 2020*].

310. Kirsten Gillibrand, *The U.S. Needs a Data Protection Agency*, MEDIUM (Feb. 12, 2020), https://medium.com/@gillibrandny/the-u-s-needs-a-data-protection-agency-98a054f7b6bf.

311. *S.3300 – Data Protection Act of 2020*, *supra* note 309.

312. Gillibrand, *supra* note 310.

313. *Id.*

314. *Id.*

315. *Id.*

digital marketplace."[316] The agency would develop and provide resources across sectors to promote data protection and privacy innovation.[317] It would also "ensure equal access to privacy protection" by protecting internet users from "'pay-for-privacy' or 'take-it-or-leave-it' provisions in service contracts."[318]

Third, the DPA would be tasked with advising Congress on the latest issues in privacy and technology, as well as educating the American government on issues like encryption and deepfakes.[319] The DPA "would also represent the United States at international forums regarding data privacy and inform future treaty agreements regarding data."[320] Unfortunately, the bill failed to capture the attention of Congress. On February 13, 2020, it was read twice before the Senate and referred to the Committee on Commerce, Science, and Transportation.[321] Because the Data Protection Act of 2020 never made it out of the Committee,[322] it died at the end of the 116th Congress.

Despite the bill's failure, its proposal was a step in the right direction. In a post titled "The U.S. Needs a Data Protection Agency," Senator Gillibrand expressed her motivations for the proposed legislation.[323] She offered two frighteningly plausible hypotheticals to illustrate how "lawlessness in the data privacy space [could] give rise to new, unexpected forms of injustice."[324] What if your health insurance company bought your fitness data from a fitness tracking app and decided to increase your rates because it thought you did not exercise enough?[325] What if tech companies could determine that you had a poor credit score, or that you were low-income?[326] And what if a third party purchased this information and used it to serve you ads for predatory payday lending schemes?[327] Many of Senator Gillibrand's concerns echo those expressed by NGOs, scholars, and think tanks specialized in the area of data privacy and protection.[328] Undeterred by the 116th Congress's lack

316. *Id.*
317. *Id.*
318. *Id.*
319. *Id.*
320. *Id.*
321. *S.3300 – Federal Data Protection*, *supra* note 300.
322. *See id.*
323. *See* Gillibrand, *supra* note 310.
324. *Id.*
325. *Id.*
326. *Id.*
327. *Id.*
328. *See supra* Sections I.A and I.C.

of enthusiasm for federal data privacy legislation, Senator Gillibrand introduced the Data Protection Act of 2021 in June 2021.[329] In a press release announcing the renewed piece of legislation, Senator Gillibrand highlighted that the new version "has undergone significant improvements, including updated provisions to protect against privacy harms and discrimination, oversee the use of high-risk data practices, and to examine and propose remedies for the social, ethical, and economic impacts of data collection."[330] She specifically identified five improvements to the proposed legislation's purpose, objectives, and functions: (1) granting the DPA oversight authority over technology mergers involving data brokers; (2) establishing an Office of Civil Rights within the DPA; (3) improving the DPA's enforcement powers; (4) prohibiting data brokers from engaging in broader categories of activities and establishing heightened penalties for certain categories of violations; and (5) promoting transparency by defining key terms like "Data Aggregators" and "Privacy Harm."[331]

While the Senate may have failed to act on Senator Gillibrand's proposed legislation in 2020, the new version has been endorsed by numerous data privacy experts working in NGOs and academic institutions.[332] Most notably, the Data Protection Act of 2021 has been lauded by Harvard Business School Professor and prominent data privacy scholar Shoshana Zuboff, who offered the following praise:

> Imagine the twentieth century without the National Labor Relations Board, the Food and Drug Administration, the Federal Deposit Insurance Corporation, the Federal Trade Commission, or any one of the dozens of critical institutions invented in that century to keep America's industrial economy safe for democracy, tethered to the rule of law and the values and principles of a democratic people. The Data Protection Act of 2021 begins the urgent work of inventing the institutions that will make our digital century safe for democracy, advancing the

329. *S.2134 – Data Protection Act of 2021*, CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/senate-bill/2134/text (last visited June 13, 2022) [hereinafter *S.2134 – Data Protection Act of 2021*].

330. *Gillibrand Introduces New and Improved Consumer Watchdog Agency to Give Americans Control over Their Data*, KIRSTEN GILLIBRAND: U.S. SENATOR FOR N.Y (June 17, 2021) [hereinafter *Gillibrand Introduces New and Improved Consumer Watchdog Agency*], https://www.gillibrand.senate.gov/news/press/release/gillibrand-introduces-new-and-improved-consumer-watchdog-agency-to-give-americans-control-over-their-data.

331. *Id.*

332. *See id.*

> democratic values of citizens' rights, the rule of law, and inclusive prosperity. With this bill, Senator Gillibrand joins a history-making new wave of legislative and regulatory efforts in the US and Europe that promise to assert democratic governance over unconstrained tech power for the sake of a digital and democratic future.[333]

As a pioneer in the realm of digital surveillance and data privacy, Professor Zuboff recognizes the importance of comprehensive federal legislation. Like its predecessor, the Data Protection Act of 2021 is before the Senate Committee on Commerce, Science, and Transportation.[334] If it does not pass both houses of Congress by the end of 2022, Senator Gillibrand will have to reintroduce a new version during the next legislative session.

2. Other Federal Legislative Proposals

Over the past couple of years, other members of Congress from both major parties have also introduced pieces of federal data privacy legislation. First, in March 2021, Representative Suzan DelBene (D-WA), a former Microsoft executive, introduced the Information Transparency and Personal Data Control Act ("ITPDCA").[335] The ITPDCA would impose several requirements on companies that the Data Protection Act of 2021 would not: (1) they would have to obtain consumers' opt-in consent before sharing personal information with third parties; (2) they would have to honor consumer requests to opt out of future collection, processing, selling, and sharing of personal information; (3) their privacy policies would have to be written clearly for consumers to understand; and (4) those that use more than 250,000 individuals' personal data per year would have to undergo a privacy audit every other year and publish the results.[336] While Senator Gillibrand's proposal suggests creating a separate agency to oversee data privacy and implement rules toward that end, the ITPDCA would delegate broad enforcement and regulatory authority to the FTC.[337] At the same time, the ITPDCA is considered "business-friendly" because it does not include a

333. *Gillibrand Introduces New and Improved Consumer Watchdog Agency*, *supra* note 330.

334. *See S.2134 – Data Protection Act of 2021*, *supra* note 329.

335. Philip J. Bezanson et al., *The Battle of the Bills Begins: Proposed Federal Data Privacy Legislation Aims to End Patchwork Problem but Increases Enforcement*, NAT'L L. REV. (Mar. 18, 2021), https://www.natlawreview.com/article/battle-bills-begins-proposed-federal-data-privacy-legislation-aims-to-end-patchwork.

336. *See id.*

337. *See id.*

private right of action and would preempt state laws.[338] Because the ITPDCA would provide much-needed clarity for businesses that are currently being forced to navigate a patchwork of state laws regulating digital privacy,[339] it has been endorsed by groups like the National Retail Federation and the U.S. Chamber of Commerce.[340] It was referred to the House Subcommittee on Consumer Protection and Commerce shortly after being introduced and has not been acted on since.[341]

Second, in May 2021, Senators John Kennedy (R-LA) and Amy Klobuchar (D-MN) introduced the bipartisan Social Media Privacy Protection and Consumer Rights Act ("SMPPCRA").[342] According to the authors, the SMPPCRA was introduced to strengthen user privacy, empower consumers to control how their data is used, and limit companies' abilities to profit from individuals' personal data.[343] This legislation would require companies to write their terms of service in plain language, allow consumers to opt out of data collection, establish mandatory notification requirements for companies within seventy-two hours of a data breach, and provide users with additional remedies when their data is compromised.[344] Like the Data Protection Act of 2021, the SMPPCRA was referred to the Senate Committee on Commerce, Science, and Transportation shortly after being introduced and has not been acted on since.[345]

---

338. *Id.*

339. *See infra* Section III.C.

340. *See* J. Craig Shearman, *Retailers Support DelBene Bill Providing Balanced Approach to Privacy Law*, NAT'L RETAIL FED. (Mar. 10, 2021), https://nrf.com/media-center/press-releases/retailers-support-delbene-bill-providing-balanced-approach-privacy-law; *U.S. Chamber Letter of Support for the Information Transparency & Personal Data Control Act*, U.S. CHAMBER COM. (Mar. 10, 2021), https://www.uschamber.com/technology/data-privacy/us-chamber-letter-of-support-the-information-transparency-personal-data-control-act.

341. *See H.R.1816 – Information Transparency & Personal Data Control Act*, CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/house-bill/1816 (last visited Apr. 8, 2022).

342. *See Kennedy, Klobuchar Introduce Bill to Protect Privacy of Consumers' Online Data*, JOHN KENNEDY: U.S. SENATOR FOR LA. (May 20, 2021), https://www.kennedy.senate.gov/public/2021/5/kennedy-klobuchar-introduce-bill-to-protect-privacy-of-consumers-online-data.

343. *See id.*

344. *Id.*

345. *See S.1667 – Social Media Privacy Protection and Consumer Rights Act of 2021*, CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/senate-bill/1667 (last visited June 13, 2022).

Third, in July 2021, Senators Roger Wicker (R-MS) and Marsha Blackburn (R-TN) introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act ("SAFE DATA Act").[346] Like the ITPDCA, the SAFE DATA Act would delegate enforcement and regulatory authority to the FTC.[347] The Act would also require the FTC to share information about discriminatory business practices with state and federal agencies; require the FTC to maintain a registry of data brokers; and empower the FTC to oversee the data practices of common carriers and nonprofits.[348] Beyond merely delegating additional authority to the FTC and giving consumers more control over how their data is collected and used, the SAFE DATA Act would require businesses to regularly assess the impacts of their data practices, especially those that pose increased risks of harm; establish internal controls and reporting mechanisms designed to mitigate risks for consumers; and prohibit data processing practices in violation of civil rights laws.[349] Like the Data Protection Act of 2021 and SMPPCRA, the SAFE DATA Act was referred to the Senate Committee on Commerce, Science, and Transportation shortly after filing and has not progressed since.[350]

Most recently, on June 3, 2022, members of the House Committee on Energy and Commerce announced a draft bipartisan federal data privacy law proposal called the American Data Privacy and Protection Act ("ADPPA").[351] The ADPPA would preempt all state data privacy laws except those in California[352] and Illinois[353] and establish a new enforcement bureau

346. *Wicker, Blackburn Introduce Federal Data Privacy Legislation*, U.S. SENATE COMM. ON COM., SCI., & TRANSP. (July 28, 2021), https://www.commerce.senate.gov/2021/7/wicker-blackburn-introduce-federal-data-privacy-legislation.

347. *See id.*

348. *Id.*

349. *Id.*

350. *See S.2499 – SAFE DATA Act*, CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/senate-bill/2499 (last visited June 13, 2022).

351. Jason C. Gavejian et al., *Congress Releases Draft Federal Data Privacy Law with Potential Traction to Pass*, JACKSON LEWIS (June 21, 2022), https://www.workplaceprivacyreport.com/2022/06/articles/consumer-privacy/congress-releases-draft-federal-privacy-law-with-potential-traction-to-pass/ [hereinafter *Congress Releases Draft Federal Data Privacy Law*].

352. *See infra* Section III.C.

353. *See Congress Releases Draft Federal Data Privacy Law*, *supra* note 351. The Illinois Biometric Information Privacy Act ("BIPA") and Genetic Information Privacy Act ("GIPA") are not discussed in this Comment because they do not provide for comprehensive data privacy protections like the other regulations, statutes, and legislative proposals discussed herein. For more information about these laws and what they do, see JACKSON LEWIS, ILLINOIS BIOMETRIC

within the FTC.[354] It would impose broad data collection and data processing requirements on a broad range of covered entities; give individual consumers rights to access, correct, and delete their personal data; prohibit companies from using data in a way that discriminates against protected classes; and require companies to submit annual impact assessments regarding how their algorithms work.[355] While Representatives Frank Pallone, Jr. (D-NJ), Cathy McMorris Rodgers (R-WA), Jan Schakowsky (D-IL), and Gus Bilirakis (R-FL) introduced the bill on June 21,[356] Senator Maria Cantwell (D-WA), who chairs the Senate Commerce Committee, and Senate Majority Leader Charles E. Schumer (D-NY) have indicated that they oppose the legislation for lacking enforcement power and generally not being robust enough.[357] Additionally, because Senator Roger Wicker (R-MS) is expected to leave the Senate Commerce Committee to lead the Senate Armed Services Committee following the 2022 midterm elections, discussions about the ADPPA and similar proposals may struggle to maintain traction going into 2023.[358]

C. State Data Privacy Laws Create a Confusing Patchwork of Requirements for Businesses to Navigate

1. California Enacted the First Comprehensive State Privacy Law in the United States in 2018

Without federal data privacy and protection legislation, states have been left to implement such laws on their own. California was the first state to pass a comprehensive data privacy law. The California Consumer Privacy Act

---

INFORMATION PRIVACY ACT FAQS, https://www.jacksonlewis.com/sites/default/files/docs/IllinoisBIPAFAQs.pdf (last visited July 15, 2022) and Joseph J. Lazzarotti & Jody Kahn Mason, *You Have Heard of the BIPA, but What About the GIPA?*, JACKSON LEWIS (Feb. 8, 2021), https://www.workplaceprivacyreport.com/2021/02/articles/gipa/you-have-heard-of-the-bipa-but-what-about-the-gipa/.

354. *See Congress Releases Draft Federal Data Privacy Law*, *supra* note 351.

355. *Id.*

356. *Press Release: E&C Announces Subcommittee Markup of Bipartisan, Bicameral Privacy Legislation & Seven Other Bills*, U.S. HOUSE COMM. ON ENERGY & COM. (June 21, 2022), https://energycommerce.house.gov/newsroom/press-releases/ec-announces-subcommittee-markup-of-bipartisan-bicameral-privacy-legislation.

357. *See* Cristiano Lima, *Top Senate Democrat Casts Doubt on Prospect of Major Data Privacy Bill*, WASH. POST (June 22, 2022, 5:53 PM EDT), https://www.washingtonpost.com/technology/2022/06/22/privacy-bill-maria-cantwell-congress/.

358. *See* Jacob Bogage & Cristiano Lima, *House and Senate Members Unveil Stalled Data Privacy Bill*, WASH. POST (June 3, 2022, 3:00 PM EDT), https://www.washingtonpost.com/technology/2022/06/03/internet-privacy-congress-compromise-proposal/.

("CCPA"), which was enacted on June 28, 2018,[359] took effect on January 1, 2020.[360] The law protects California residents from harmful data practices by regulating for-profit entities (including data brokers[361]) doing business in California that fall into at least one of three categories.[362] A company must either (1) have annual gross revenues of more than $25 million; (2) buy, receive, sell, or share the personal information of more than 50,000 consumers, households, or devices (either in one category or across all categories); or (3) derive at least 50% of its annual revenues from sales of consumers' personal information.[363] The CCPA does not apply to the government or non-profit entities.[364]

The CCPA, though much more limited in scope, drew inspiration from the European Union's GDPR[365] and aims to secure four main privacy rights for California citizens.[366] First, the CCPA gives Californians the right to know what "personal information a business collects about them and how it is used and shared."[367] If a California consumer requests their information from a company, it must disclose what information was collected, how it was used, and if it was shared or sold.[368] The consumer may also specifically request that a business disclose the following:

> The categories of personal information collected[;] Specific pieces of personal information collected[;] The categories of sources from which the business collected personal information[;] The purposes for which the business uses the personal information[;] The categories of third parties with whom the business shares the personal information[;] [and] The categories

359. *See* LAURA JEHL & ALAN FRIEL, CCPA AND GDPR COMPARISON CHART (2018) (Westlaw, Practical Law: Overview W-016-7418).

360. *Id.*; Zack Whittaker, *Silicon Valley Is Terrified of California's Privacy Law. Good.*, TECHCRUNCH (Sept. 19, 2019, 11:00 AM CDT), https://techcrunch.com/2019/09/19/silicon-valley-terrified-california-privacy-law/.

361. *See California Consumer Privacy Act (CCPA)*, OFF. ATT'Y GEN., https://oag.ca.gov/privacy/ccpa (last visited Jan. 8, 2022).

362. *See* GDPR VS CCPA, *supra* note 270, at 2.

363. California Consumer Protection Act of 2018, CAL. CIV. CODE § 1798.140(c)(1) (West 2018).

364. *California Consumer Privacy Act (CCPA)*, *supra* note 361.

365. JEHL & FRIEL, *supra* note 359.

366. *See California Consumer Privacy Act (CCPA)*, *supra* note 361.

367. *Id.*

368. *Id.*

> of information that the business sells or discloses to third parties[.][369]

Second, with some exceptions, the CCPA gives consumers "[t]he right to delete personal information collected from them."[370] Third, the law codifies "[t]he right to opt-out of the sale of their personal information."[371] And fourth, it provides consumers with "[t]he right to non-discrimination for exercising their CCPA rights."[372]

The above rights are granted to California consumers by requiring businesses to comply with new rules under the CCPA. The law requires covered entities to provide links on their websites that allow consumers to opt out of the sale and disclosure of their personal data.[373] The California Attorney General clarified that this process should be easy for consumers and that opting out should require only minimal steps.[374] Such links may be labeled "Do Not Sell My Personal Information" or "Do Not Sell my Info."[375] Businesses have fifteen business days to comply with opt-out requests and forty-five days to comply with requests to know or delete user information.[376] If businesses fail to comply with such requests in a timely manner, they may be fined up to $7,500 per violation.[377]

For most CCPA violations, California consumers are not entitled to bring private lawsuits against the businesses that harmed them.[378] In fact, in the instance of most CCPA violations, the only action available to consumers is to file a consumer complaint with the Office of the Attorney General.[379] The Attorney General, who does not represent individual California consumers, may use such "complaints and other information . . . [to] identify patterns of misconduct that may lead to investigations and actions on behalf of the collective legal interests of the people of California."[380] In practice, this will likely mean that only the most egregious and repetitive violators of the law

369. *Id.*
370. *Id.*
371. *Id.*
372. *Id.*
373. GDPR VS CCPA, *supra* note 270, at 3.
374. *Id.*
375. *Id.*
376. *Id.*
377. *See* Kamal, *supra* note 305.
378. *See California Consumer Privacy Act (CCPA)*, *supra* note 361 (explaining how consumers can sue a business under the CCPA for data breaches only, either to obtain statutory damages or compensation of actual monetary damages).
379. *Id.*
380. *Id.*

will face any sort of repercussions due to the time and resource constraints placed on the Office of the Attorney General.

Although the CCPA helps to fill the void created by a lack of federal legislation, it has been criticized for its shortcomings. First, while the law requires covered entities to offer consumers an opt-out feature, opting out "only stops the *selling* of personal information, and it does not impact other uses of their information."[381] As explained in Part I above, technology companies typically do not *sell* user data, but instead license access to it.[382] Because there is often no sale of the data itself, the right to opt-out from companies like Facebook and Google may be rendered completely ineffective.

Second, although consumers have a right to request that their data be deleted, many of the law's loosely defined exceptions permit businesses to deny their requests.[383] The Office of the Attorney General lists several common reasons that allow businesses to lawfully keep a consumer's personal information even after receiving a deletion request.[384] For example, the business may not be able to verify a consumer request, or it may need to keep the information to complete a transaction, provide a product or service, or communicate warranty or product recall information.[385] Other businesses may need to maintain consumer information pursuant to business security practices, or for other internal uses that align with consumers' reasonable expectations for use, based on the context in which the information was provided.[386] Finally, a business may need to use such information to comply with various legal obligations, to exercise legal claims or rights, or to defend against legal claims.[387]

If a business denies a California consumer's deletion request, the Office of the Attorney General advises the consumer to follow up with the business to ask for its reasons.[388] Because the above exceptions provide such broad categories for an entity to justify not deleting information, it is likely that this right will be difficult to enforce in practice. While the CCPA was a step in the right direction toward protecting the data privacy rights of some Americans, its many flaws make it a problematic model for other states to

381. GDPR VS CCPA, *supra* note 270, at 3 (emphasis added).
382. *See supra* Part I.
383. *See California Consumer Privacy Act (CCPA)*, *supra* note 361.
384. *See id.*
385. *Id.*
386. *Id.*
387. *Id.*
388. *Id.*

turn to when drafting their own state legislation. Fortunately for California consumers and legislators seeking inspiration for their own data privacy laws, the framework established by the CCPA has been updated since the law went into effect in January 2020.

2. California Voters Approved Proposition 24 in 2020 to Cure Major Deficiencies Contained in the CCPA

In November 2020, California voters approved Proposition 24, a ballot measure designed to overhaul the framework established by the CCPA.[389] Proposition 24, more commonly known as the California Privacy Rights Act of 2020 ("CPRA"), expanded California consumers' control over their personal information and established new requirements for businesses that fall within its scope.[390] While the CPRA does not go into full effect until January 1, 2023, it immediately created the California Privacy Protection Agency ("CalPPA"), which is responsible for "implementing and enforcing the CCPA and . . . CPRA."[391]

The CPRA will apply to a slightly different subset of for-profit businesses that do business in California and process Californians' personal information. While the CCPA applies to businesses that either have revenues over $25 million; buy, sell, or share more than 50,000 California consumers' or households' personal information; or derive 50% or more of their revenues from selling consumers' information, the CPRA increased the threshold to 100,000 consumers or households and applies to businesses that derive 50% of their revenue from selling *or sharing* personal information.[392] This expanded scope helped close the loophole identified above whereby businesses could avoid the requirements of the CCPA by "sharing" consumer data with third parties, rather than "selling" the data. Accordingly, once the CPRA goes into effect, covered entities that share enough user information will be required to give consumers the right to opt out of information sharing practices.[393]

---

389. Sam Dean, *California Voters Approve Prop. 24, Ushering in New Rules for Online Privacy*, L.A. TIMES (Nov. 4, 2020, 10:43 AM PT), https://www.latimes.com/business/story/2020-11-03/2020-california-election-tracking-prop-24.

390. *See* Peter Hegel et al., *The California Privacy Rights Act (CPRA) Has Been Enacted into Law*, PAUL HASTINGS (Nov. 6, 2020), https://www.paulhastings.com/insights/ph-privacy/blog-the-california-privacy-rights-act-cpra-has-been-enacted-into-law.

391. *Id.*

392. *See California Privacy Rights Act Passes – Dramatically Altering the CCPA*, MINTZ (Nov. 6, 2020), https://www.mintz.com/insights-center/viewpoints/2826/2020-11-06-california-privacy-rights-act-passes-dramatically.

393. *See id.*

The CPRA will also restrict the disclosure and use of Californians' "sensitive personal information," expand the CCPA's private right of action, impose new limits on data collection and retention functions, and establish new consumer rights.[394] When a covered entity collects or uses consumers' financial information, log-in credentials, precise location data, private communications, genetic information, biometric information, health information, or similarly "sensitive" categories of information, its use of that information will be limited to those purposes that an average consumer using the company's good or service would expect.[395] While the CCPA's private right of action is limited to instances where a covered entity fails to utilize appropriate security measures (as opposed to privacy measures) and falls victim to a breach compromising consumers' sensitive personal information (a term not defined in the CCPA[396]),[397] the CPRA expands the private right of action to include privacy violations involving the unauthorized collection, use, or processing of email addresses, security questions, and passwords.[398] While the CCPA "did not explicitly address data retention," the CPRA prohibits storing personal information beyond a "reasonably necessary" time and restricts collection, use, and sharing of information in ways that are disproportionate to the original purposes underlying the business' collection or processing.[399] In addition to all of these improvements, the CPRA grants consumers a right to correct inaccurate information.[400] While the CPRA contains significantly improved consumer protection measures relative to the CCPA, businesses that meet one of the three CPRA thresholds may find themselves scrambling to comply with its requirements as the January 1, 2023, effective date approaches. At a February 2022 CalPPA Board meeting, the agency's Executive Director announced that the regulations implementing the provisions of the CPRA may not be finalized until the end of the year.[401] Accordingly, businesses will be forced to update their privacy

394. *Id.*

395. *Id.*

396. *See* David Stauss et al., *How Do the CPRA, CPA & VCDPA Treat Sensitive Personal Information?*, BYTE BACK (Feb. 16, 2022), https://www.bytebacklaw.com/2022/02/how-do-the-cpra-cpa-and-vcdpa-treat-sensitive-personal-information/ ("The current California Consumer Privacy Act (CCPA) does not define or treat differently sensitive information.").

397. Jena M. Valdetero & David A. Zetoony, *CCPA Litigation Up 44.1%*, 12 NAT. L. REV. (Mar. 7, 2022), https://www.natlawreview.com/article/ccpa-litigation-441.

398. *See California Privacy Rights Act Passes – Dramatically Altering the CCPA*, *supra* note 392.

399. *Id.*

400. *Id.*

401. Clayton G. Northouse et al., *California Privacy Agency: CPRA Regs Not Likely Until*

and security practices with just weeks or months of advance notice.[402] While the CalPPA will not start enforcing the CPRA until July 1, 2023,[403] the speed with which businesses will be forced to overhaul their operations will likely lead to increased business resistance to (and lobbying against) subsequent state or federal laws regulating their privacy practices. To earn the support of the business community, federal legislative proposals should ensure ample time for affected businesses to reform their data practices.

3. Other Recently Adopted State Data Privacy Laws Force Companies to Navigate a Complicated Patchwork of Regulation

While California has had the most success with regulating data and technology companies' collection and use of users' personal data, state legislatures across the United States are ramping up their efforts to fill the gap left by the absence of federal law. While only two data privacy laws were introduced in state legislatures in 2018, more than 100 such bills were introduced in at least thirty-eight states in 2022.[404] The significant majority of these bills failed before passage, but the uptick in attempts to legislate in this space indicates that state governments are finally beginning to understand the urgency of action. As public awareness about the role that data and technology companies play in collecting, storing, processing, and sharing personal data has started to increase in recent years, it was only a matter of time before more states succeeded in implementing their own regulatory frameworks.

In addition to California, four states have passed comprehensive data privacy laws that are scheduled to take effect in 2023: Colorado, Connecticut, Utah, and Virginia.[405] Although none of these laws have yet taken effect, key provisions of the Colorado Privacy Act and Virginia Consumer Data Protection Act, both of which passed in 2021 and were modeled after the California laws, have been compared to the CCPA and CPRA at length.[406]

Late 2022, SIDLEY AUSTIN: DATA MATTERS (Feb. 23, 2022), https://datamatters.sidley.com/california-privacy-agency-cpra-regs-not-likely-until-late-2022.

402. *See id.*

403. *Id.*

404. *See* David McCabe & Cecilia Kang, *As Congress Dithers, States Step in to Set Rules for the Internet*, N.Y. TIMES (May 14, 2021), https://www.nytimes.com/2021/05/14/technology/state-privacy-internet-laws.html.

405. *See State Laws Related to Digital Privacy*, NAT'L CONF. STATE LEGISLATURES (June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (highlighting California, Colorado, Connecticut, Utah, and Virginia as states that have enacted "comprehensive" data privacy laws).

406. *See 2023 State Privacy Guide*, BYTE BACK, https://www.bytebacklaw.com/category/

Although this Comment does not address the specific differences between the California and other state laws, variations in their texts only reinforce the notion that state attempts to regulate in the absence of federal action are creating a patchwork of contradictory obligations that complicate businesses' attempts to comply with an ever-changing regulatory landscape. As these laws take effect and more states pass their own versions of laws imposing contradictory obligations on companies, the necessity of federal legislation will only grow more apparent. The federal government must act now to provide uniform standards for protecting consumers' right to online privacy.

In the future, both state and federal legislators may instead turn to another, surprising state for a more progressive framework regulating data privacy: Oklahoma.

D. The Oklahoma Computer Data Privacy Act

Oklahoma was one of the first states in the nation to propose groundbreaking opt-in data privacy legislation.[407] First introduced in January 2021,[408] HB 1602 was filed to create the Oklahoma Computer Data Privacy Act ("OCDPA"), a bipartisan bill that would have required "internet technology companies to obtain explicit permission to collect and sell personal data."[409] The bill was introduced by Representative Josh West, a Republican,[410] and Representative Collin Walke, a Democrat.[411] The OCDPA was referred to the Republican-led House Technology Committee on February 2, 2021.[412] By the time the bill unanimously passed out of committee on February 10, it had forty-two total co-authors, and a Senate version of the bill had been drafted with bipartisan support.[413]

2023-state-privacy-guide/ (last visited June 29, 2022) (introducing a ten-week series highlighting similarities and differences between the CCPA, CPRA, Colorado Privacy Act, and Virginia Consumer Data Protection Act, especially regarding treatment of different categories of data, opt-out requests, consumer requests, data processing agreements, and sales of user data).

407. *Opt-In Data Privacy Legislation Passes Committee*, OKLA. STATE LEGISLATURE (Feb. 10, 2021, 12:51 PM), https://www.okhouse.gov/Media/News_Story.aspx?NewsID=7884.

408. *See Bill Information for HB 1602*, OKLA. STATE LEGISLATURE, http://www.oklegislature.gov/BillInfo.aspx?Bill=hb1602&Session=2100 (last visited June 13, 2021).

409. *Opt-In Data Privacy Legislation Passes Committee*, *supra* note 407.

410. *Representative Josh West: District 5 - Republican*, OKLA. STATE LEGISLATURE, https://www.okhouse.gov/Members/District.aspx?District=5 (last visited Jan. 8, 2022).

411. *Representative Collin Walke: District 87 - Democrat*, OKLA. STATE LEGISLATURE, https://www.okhouse.gov/Members/District.aspx?District=87 (last visited Jan. 8, 2022).

412. *See Bill Information for HB 1602*, *supra* note 408.

413. *See id.*

While some of the OCDPA's structural aspects resembled those of the CCPA, the OCDPA was more protective of Oklahomans' data privacy rights in nearly every possible way. The proposed legislation would have protected Oklahoma residents from the "wrong and harmful"[414] practices of large businesses that profit from Oklahomans' personal information.[415] The OCDPA would have regulated any business that

> a. does business in this state,
> b. collects consumers' personal information or has that information collected on the business's behalf,
> c. alone or in conjunction with others, determines the purpose for and means of processing consumers' personal information, and
> d. satisfies one or more of the following thresholds:
> (1) has annual gross revenue in an amount that exceeds Ten Million Dollars ($10,000,000.00),
> (2) alone or in combination with others, annually buys, sells, or receives or shares for commercial purposes the personal information of fifty thousand or more consumers, households or devices, or
> (3) derives twenty-five percent (25%) or more of the business's annual revenue from selling consumers' personal information.[416]

Like the CCPA, the OCDPA would not have regulated government or non-profit entities.[417]

The Oklahoma Computer Data Privacy Act would have secured four main privacy rights for Oklahomans. First, it would have established a right to request that a business disclose "the categories and specific items of personal information" that a business has collected about consumers.[418] Second, it would have given consumers the right to request that a business delete any personal information that it has collected.[419] Third, it would have created a

414. *Opt-In Data Privacy Legislation Passes Committee*, *supra* note 407.

415. *See generally* H.B. 1602, 58th Leg., 1st Sess. § 2(13) (Okla. 2021) (defining the term "personal information" broadly to include "information that identifies, relates to, describes, can be associated with or can reasonably be linked to, directly or indirectly, a particular consumer or household").

416. *Id.* § 3(A)(1).

417. *See id.* § 2(3).

418. *Id.* § 11(A).

419. *Id.* § 12(A).

right to request that a business that sells or shares consumers' personal information disclose the categories of information collected, the categories of information sold or shared, and the categories of third parties to whom the information was sold or shared.[420] Finally, the proposed legislation would have established the right to opt out of the sale of personal information by directing the business to not sell the information.[421] Each of these rights would have applied in addition to the requirement that Oklahoma consumers would need to opt in to data collection practices in the first place.[422]

The above rights would have been granted to Oklahoma residents by requiring businesses to behave in accordance with rules and procedures established by the Oklahoma Corporation Commission ("OCC").[423] The proposed bill would have required the Commission to implement four main categories of rules and procedures. First, the OCC would develop procedures that govern "the determination of, submission of, and compliance with" verified consumer requests for information.[424] Second, it would create rules to "facilitate and govern the submission of and compliance with a request to opt out or opt in to the sale of personal information."[425] Third, and most interestingly, the OCC would be tasked with developing a "recognizable and uniform opt-in logo or button for use on the businesses' Internet websites in a manner that promotes consumer awareness of the opportunity to opt in to the sale of personal information."[426] And fourth, the OCC would establish guidelines and procedures to ensure that the information and notices that businesses are required to provide are (1) easy for the average consumer to understand, (2) accessible to users with disabilities, and (3) available in the language the consumer uses to interact with the business.[427]

The bill's primary authors, Representatives West and Walke, viewed this legislation as a way for Oklahomans to "reclaim their privacy that was wrongfully taken from them."[428] When the bill was still in its early stages, its authors were confident that it had a high chance of success because consensus

420. *Id.* § 13(A).
421. *Id.* § 14(A).
422. *See id.* § 14(C).
423. *See id.* § 9(A).
424. *Id.* § 9(B)(1).
425. *Id.* § 9(B)(2).
426. *Id.* § 9(B)(3).
427. *Id.* § 9(B)(4).
428. *See* Sasha L. Beling & Zachary A.P. Oubre, *What You Need to Know About Data Privacy and Cybersecurity: Oklahoma Computer Data Privacy Act*, MCAFEE & TAFT.TV (Feb. 11, 2021), https://www.mcafeetaft.com/what-you-need-to-know-about-data-privacy-and-cybersecurity-oklahoma-computer-data-privacy-act/.

was starting to grow around the notion that data privacy is "not [a] partisan issue."[429] According to Walke, it is time "to let Oklahomans have their privacy."[430] Despite the authors' confidence and the bill's broad support in the Oklahoma House of Representatives, the OCDPA failed to make it out of the Senate Judiciary Committee by the 2021 deadline.[431]

While HB 1602 did not make it out of the Senate in 2021, Representatives West and Walke introduced HB 2969 ahead of the 2022 legislative session.[432] The text of HB 2969 was nearly identical to that of HB 1602, subject to four minor changes. First, as amended, HB 2969 updated the definitions section of the OCDPA by (a) removing "DNA" from the scope of "biometric information" and placing it in the new "genetic information" category and (b) defining "pseudonymization" in a similar way as the GDPR.[433] Second, HB 2969 increased the revenue threshold from $10 million to $15 million.[434] Third, HB 2969 included nonprofit radio and television programming in the scope of "noncommercial activities" that would not be subject to the OCDPA.[435] Fourth, HB 2969 would have explicitly required covered entities to gain consumer consent, as defined in Section 2(22), before they could be deemed to have opted into collection or sale of their personal data.[436]

Like HB 1602, HB 2969 passed the House Technology Committee and the full House.[437] HB 2969 was then sent to the Senate with limited time to pass before the end of the 2022 legislative session.[438] Because HB 2969 failed to pass the full Senate before the April 14 deadline, it too died.[439] Following

---

429. *See id.*

430. *Id.*

431. *See* David Stauss, *Status of Proposed CCPA-Like State Privacy Legislation as of April 12, 2021*, BYTE BACK (Apr. 12, 2021), https://www.bytebacklaw.com/2021/04/status-of-proposed-ccpa-like-state-privacy-legislation-as-of-april-12-2021/.

432. *See Bill Information for HB 2969*, OKLA. STATE LEGISLATURE, http://www.oklegislature.gov/BillInfo.aspx?Bill=hb2969&Session=2200 (last visited June 13, 2022).

433. *See* H.B. 2969, 58th Leg., 2nd Sess. §§ 2(2), 2(10), 2(16) (Okla. 2022) (engrossed).

434. *See id.* § 3(A)(1)(d)(1).

435. *Id.* § 5(3).

436. *See id.* §§ 13(C)(1)(c), 16(C); *see also id.* § 2(22) (defining consent as "an act that clearly and conspicuously communicates the individual's authorization of an act or practice that is made in the absence of any mechanism in the user interface that has the purpose or substantial effect of obscuring, subverting or impairing decision-making or choice to obtain consent").

437. *See Bill Information for HB 2969*, *supra* note 432.

438. *See* David Stauss, *Proposed State Privacy Law Update: May 9, 2022*, BYTE BACK (May 8, 2022), https://www.bytebacklaw.com/2022/05/proposed-state-privacy-law-update-may-9-2022/#more-3903.

439. *See id.*

Representative Walke's announcement that he will not seek reelection in 2022,[440] the future of data privacy legislation in Oklahoma is somewhat uncertain. While Representative Walke's efforts over the past two years have propelled Oklahoma into the national conversation surrounding the regulation of data and technology companies' privacy practices, it remains to be seen whether another state legislator will step up and continue his fight during the 2023 legislative session.

As regulatory efforts have ramped up, few companies have taken note. As the next section explains, while some companies have taken steps to make their businesses more privacy friendly, their action alone falls short of affecting meaningful industrywide change.

E. The Privacy Premium for Data Protection

As society has begun peeking behind the "digital curtain" that once obscured Big Data's industry practices from the public, some companies have taken steps to give users more control over their data.[441] YouTube, for example, updated its Terms Service in January 2022 to provide more "transparency" to the platform's users, purporting to improve the legal document's readability.[442] However, when I analyzed the updated language using two publicly available online tools, I found that the nearly four-thousand-word document is only "easily understandable" upon first read by a person with a graduate-level education. It would take the average person a full twenty minutes to read. Despite YouTube's underwhelming attempt at improving its transparency, there is one technology company that has done more to protect its users' data privacy than any other: Apple.

Apple has long championed data privacy reform. In 2010, Apple's former CEO and co-founder Steve Jobs warned an audience at the All Things Digital Conference about privacy issues:

> Privacy means people know what they're signing up for, in plain English and repeatedly . . . . I believe people are smart and some people want to share more data than other people do. Ask them.

---

440. *See Oklahoma State Rep. Collin Walke Announces He Won't Seek Reelection for H.D. 87, Endorses Ellyn Hefner*, OKLA. CITY SENTINEL (Apr. 14, 2022), https://www.city-sentinel.com/government/oklahoma-state-rep-collin-walke-announces-he-won-t-seek-reelection-for-h-d-87/article_a00466ea-bc19-11ec-8548-977ea664cc32.html.

441. Hossein Rahnama & Alex "Sandy" Pentland, *The New Rules of Data Privacy*, HARV. BUS. REV. (Feb. 25, 2022), https://hbr.org/2022/02/the-new-rules-of-data-privacy.

442. News9 Staff, *YouTube Announces Updated Terms of Service, Will Come into Effect January 5*, NEWS NINE (Nov. 24, 2021, 11:40 PM), https://www.news9live.com/technology/app-news/youtube-terms-of-service-january-5-136128.

> Ask them every time. Make them tell you to stop asking them if they get tired of your asking them. Let them know precisely what you're going to do with their data . . . .[443]

Interestingly, Mark Zuckerberg sat in this audience.[444]

While Apple has famously protected its users by refusing to give U.S. law enforcement agencies backdoor access to iPhones,[445] it sent shockwaves through the Big Data industry when it released its iOS 14.5 software update in April 2021. One of the most important features introduced was a new privacy tool called App Tracking Transparency.[446] The update shows iPhone and iPad users a pop-up notification when they open an app that tracks them and shares their data with third parties,[447] prompting users to opt in to allow apps like Facebook to track them.[448] Ahead of iOS 14.5's launch, Apple released "A Day in the Life of Your Data," a thorough but easy-to-read report showing users how companies collect and use their data and how Apple's new privacy features allowed them to regain some control over their personal information.[449] The day after the report's release, Apple CEO Tim Cook reiterated the company's stance on data privacy in a keynote address at the Computers, Privacy and Data Protection conference:

> Technology does not need vast troves of personal data, stitched together across dozens of websites and apps, in order to succeed. . . . Advertising existed and thrived for decades without it. And we're here today because the path of least resistance is rarely the path of wisdom. If a business is built on misleading

443. Kaya Yurieff, *Steve Jobs Warned About Privacy Issues in 2010. Mark Zuckerberg Was in the Audience*, CNN (Mar. 27, 2018, 2:14 PM ET), https://money.cnn.com/2018/03/27/technology/steve-jobs-mark-zuckerberg-privacy-2010/index.html.

444. *Id.*

445. *See* Michelle Quinn, *Apple's Refusal to Create IPhone Backdoor Pits Public Safety Against Personal Privacy*, VOA (Jan. 15, 2020, 7:25 AM), https://www.voanews.com/a/silicon-valley-technology_apples-refusal-create-iphone-backdoor-pits-public-safety-against-personal/6182601.html.

446. *See* Rebecca Heilweil, *Why the New IOS Update is Such a Big Deal*, VOX (Apr. 26, 2021, 10:52 AM EDT), https://www.vox.com/recode/22393931/facebook-ios-14-5-app-tracking-transparency-iphone-privacy.

447. *See id.*

448. *See* Matthew Fox, *$315 Billion in Market Value Has Been Erased from These 4 Companies Since Apple's IOS Privacy Changes Went into Effect Last Year*, MKTS. INSIDER (Feb. 3, 2022, 10:02 AM), https://markets.businessinsider.com/news/stocks/facebook-meta-stock-apple-idfa-ios-privacy-change-social-media-2022-2.

449. *See* APPLE, INC., A DAY IN THE LIFE OF YOUR DATA: A FATHER-DAUGHTER DAY AT THE PLAYGROUND (2021), https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf.

> users, on data exploitation, on choices that are no choices at all, then it does not deserve our praise. It deserves reform.[450]

Apple's iOS 14.5 privacy update was not a step, but a leap in the right direction. In the first two weeks following iOS 14.5's release, only around 4% of Americans opted in to app tracking.[451] And companies that relied on app tracking as their main source of revenue felt the blow. In less than a year after Apple's iOS 14.5 privacy tools went into effect, social media companies Facebook, Snap, Twitter, and Pinterest together lost $315 billion in market value.[452] Facebook alone lost over $200 billion in market value and $10 billion in ad revenue as a direct result of Apple's update.[453]

Despite these impressive figures, the tech titans still triumph. Both Facebook and Google reported "strong growth in their ad business for the fourth quarter of 2021."[454] Facebook's overall ad revenue still grew by more than $30 billion from 2020 to 2021, and its ad revenue for the fourth quarter of 2021 "jumped 20% year-on-year . . . despite concerns brought about by Apple's iOS14 changes."[455]

What these numbers communicate is clear: while Apple's moves are commendable, the company cannot singlehandedly change its competitors' incredibly profitable business practices. Leaving industry change up to Apple alone is not a solution. While the company's update helped protect its consumers' data privacy across most Apple devices, tens of millions of Americans remain unprotected. In May 2022, Apple's iOS commanded 57.43% of the mobile operating system market in the U.S., while Google's Android accounted for 42.29%.[456] While Android holds a smaller market share, Android smartphones are significantly more affordable than their Apple counterparts. In 2019, the iPhone's average selling price ("ASP") was

---

450. Sara Morrison, *Why Facebook and Apple Are Fighting over Your Privacy*, VOX (Feb. 1, 2021, 12:16 PM EST), https://www.vox.com/recode/22254815/facebook-apple-privacy-ios-14-lawsuit.

451. Ben Lovejoy, *Unsurprisingly, Almost No Americans Are Opting in to App Tracking*, 9TO5MAC (May 7, 2021, 5:07 AM PT), https://9to5mac.com/2021/05/07/opting-in-to-app-tracking/.

452. Fox, *supra* note 448.

453. *See id.*

454. Janice Tan, *Meta and Alphabet Continue to See Strong Growth in Ad Business*, MKTG-INTERACTIVE (Feb. 3, 2022), https://www.marketing-interactive.com/google-facebook-advertising-earnings.

455. *See id.*

456. *Mobile Operating System Market Share United States of America: May 2021 – Mar May 2022*, GLOB. STATS, https://gs.statcounter.com/os-market-share/mobile/united-states-of-america (last visited June 13, 2022).

nearly $800, "almost three times higher than the overall industry average."[457] In 2021, the iPhone's U.S. ASP climbed up to $873.[458] In effect, what exists now is a data privacy premium—where the people best equipped to protect their data privacy are those who can afford it.

In the absence of regulation, companies have been left to their own devices. While a handful have taken it upon themselves to protect their users' data, the largest and worst offenders continue to wield outsized power over one of society's most valuable resources. It is imperative that lawmakers work together to create a framework that provides all Americans with a fair and equal opportunity to safeguard their data.

IV. Recommendations for Policymakers

Without a comprehensive federal law regulating data privacy and protection in the United States, American consumers will continue to suffer at the hands of Big Data. The current lack of regulation privileges the rights of gigantic technology companies and data brokers over the protection of society as a whole. When left unregulated, these markets undermine freedom and democracy.[459]

This Part proposes solutions that policymakers should implement to protect the rights of Americans against harmful data practices perpetrated by technology and data companies. First, it calls for sweeping federal data privacy reform by way of a comprehensive federal data privacy law. It then proposes specific details, derived from the most promising aspects of existing privacy laws and proposals, that policymakers should include in such legislation, including universal opt-in requirements. Finally, it explores possible enforcement mechanisms, suggesting the creation of the Data Protection Agency.

A. Enact a Federal Data Privacy Law

While some U.S. states are taking the right steps toward protecting data privacy by implementing state laws, creating a patchwork of different state laws for companies to follow is not a viable long-term solution. A federal

457. Donna Fuscaldo, *Apple's World Smartphone Market Share Above 50%*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/news/apple-global-smartphone-market-share-more-50-first-time/.

458. Ina Fried, *Average U.S. IPhone Price Hits a Record $873*, AXIOS (Jan 25, 2021), https://www.axios.com/iphone-price-12-cost-apple-e54d9f74-9933-4d3d-91ec-440900cf755f.html.

459. *See* THE SOCIAL DILEMMA, *supra* note 28, at 1:24:22 (explaining how these markets should even be outlawed because "they have inevitable destructive consequences").

law is necessary for both uniformity for consumers and easier compliance for companies. A uniform law for consumers would make Americans aware of the harmful data practices currently in effect, protect their data privacy rights, and empower them to exercise those rights. A federal law would also benefit businesses. Without a federal law in place, states will continue to enact contradictory legislation and further complicate companies' compliance efforts.

Assume that the OCDPA passes in 2023 and goes into effect later that year. While it shares some similarities with the CCPA and CPRA, it importantly requires opt-in, not opt-out, consent. It also applies to a significantly higher number of companies than do the California laws. Companies that operate in Oklahoma that adopted policies consistent with California's legislation would be required to update their policies to satisfy the Oklahoma requirements. In effect, because it is impractical for companies to create different versions of their businesses to operate in each state, California companies would impose the more stringent requirements of the Oklahoma law on California consumers without providing them with the same rights.

Now imagine that over the next few years, ten more states adopt their own privacy laws with different requirements. Some require opt-in consent, while others do not. Some apply to businesses with annual revenues over $5 million, while others apply to all businesses, including non-profit organizations. Some provide the right to have data deleted, and others offer their citizens less expansive rights. Some apply to residents within state boundaries, while others apply to state citizens regardless of their location. Companies will be stuck in a loop, being forced to constantly change to ensure compliance with each state's contradictory requirements. A uniform federal law would remedy the problems that a patchwork system of data privacy laws would create by establishing a consistent set of rules for everyone to follow, in turn lowering the costs of compliance.

B. What a Federal Data Privacy Law Should Include

This section outlines seven key elements policymakers should include and consider in drafting a federal data privacy law.

1. The Scope of Protection

The scope of this law should be territorially based. Like the GDPR, any person who is physically present within the borders of the United States would be afforded protection under the law. This model is superior to the citizen-based applications of the CCPA/CPRA and the OCDPA because it is

easier for companies to enforce. Instead of requiring companies to follow U.S. citizens around the world, this law would allow companies to adopt uniform compliance practices for all operations within the boundaries of the United States.

2. Regulations for Businesses

At a minimum, this law should regulate (1) for-profit entities (2) operating in the United States that (3) either (a) have an annual revenue over $15 million; (b) buy, sell, receive, or share the personal data or information of 50,000 or more consumers, devices, or households; or (c) make at least 25% of their annual revenue from selling personal data or information. Like California's legislation, this law should apply both online and offline and should specifically apply to data brokers that do not already fall within the scope of the FCRA.

3. Default Opt-in Requirements

This law should require businesses to permit consumers to opt in, rather than opt out of data collection. By forcing companies to make data privacy—not data collection—the default, consumers would be afforded more control over their data privacy. In addition, policymakers should develop guidelines similar to those suggested in the OCDPA and require businesses' websites to include a standardized button or logo designed to promote consumer awareness of their ability to opt in.

4. Federal Preemption

Like the ITPDCA, this federal framework must preempt all state data privacy laws. While the ADPPA would preempt all comprehensive state law counterparts except California's, allowing even one state framework to remain in effect would only serve to continue imposing contradictory obligations on businesses.

5. Readable Terms and Conditions

The law should also compel all eligible businesses to rewrite their terms and conditions of service and privacy policies in language that is easily understandable to the average American. While the upfront costs to companies to implement such changes will be high, they will decrease as larger companies lead the charge. The companies must be made to bear these costs because the current models are designed to prevent the vast majority of the population from understanding what they are surrendering when clicking "I agree." And these are not impossible changes for companies to implement.

The British Broadcasting Corporation serves as a great model because it has some of the most straightforward and readable language of any large company.[460] By requiring service and privacy policies to be readable, policymakers can level the playing field between society and Big Data and empower consumers to knowingly and willingly consent to the collection and use of their data.

6. Transparency Requirements

The law should require businesses to be transparent with consumers in three main ways. First, businesses should, at a minimum, disclose what information they collect on individuals, how they use that information, with whom the information is shared, and how long it is stored. Second, companies should be required to be transparent about subsequent policy updates. They should be required to provide users with a clear and concise explanation of how new policies or terms are different, allowing users to consistently make meaningful and educated decisions about how they want to manage their data. Third, businesses (especially social media platforms) should be required to disclose to consumers if their platforms use content-shaping algorithms and explain how those algorithms shape the content and information that users see. This would accomplish two main goals. First, people would be made aware that such algorithms exist and have been informing the information they consume on those platforms. Second, this would empower consumers to make informed decisions about the variety of information they want to see online, instead of the default being personalized news and content.

7. Data Privacy Rights for Americans

Finally, the law should grant consumers the following rights: (1) the right to request data; (2) the right to have their data deleted after it has been used; (3) the right to correct data; (4) the right to revoke consent to data collection or use at any time; (5) the right to see how a company has categorized them; and (6) the right to see with whom their data has been shared and to whom it has been sold.

C. Enforcement: The Data Protection Agency

Federal data privacy legislation should establish an independent federal agency that would implement and enforce data privacy rules and regulations. Senator Gillibrand's proposed DPA is an excellent model for what this

460. *See generally supra* notes 155–56 and accompanying text.

should look like.[461] This section relies heavily on Senator Gillibrand's proposals.[462]

The DPA would serve three core missions. First, it would enforce data protection rules, handle complaints of violations, conduct investigations for alleged violations, and inform the public on matters related to data protection, including by creating a data broker registry like the one proposed in the SAFE DATA Act. Second, it would ensure fair competition within the digital marketplace by developing and providing resources across sectors to promote innovation on data privacy and protection fronts and ensure equal access to privacy protection. Like the SAFE DATA Act and the ADPPA, it would ensure that data processing practices do not violate civil rights law. Third, it would keep Congress apprised of issues in privacy technology and represent the United States on the international stage by attending international data privacy forums.

By creating a central agency to handle such matters, the United States would avoid many of the problems that the EU enforcement agencies first faced under the GDPR. Without a federal agency in place to enforce data privacy regulations and to handle complaints, the bulk of the work would fall on state attorneys general, corporation commissions, and other potentially underfunded state agencies. Unfortunately, neither these agencies nor the FTC have the capabilities or specialized training to oversee data privacy enforcement at scale. A decentralized, state-based system would mean that some states would be forced to do a disproportionate amount of work, putting them in the same position as the Irish Data Protection Commission. If that were the case, enforcement would fall short, and most Americans would not enjoy equal rights to data privacy.

While technology and data companies will resist a federal privacy law that subjects them to oversight by a new federal agency, our data, our privacy, and our freedom are at stake. These companies have a responsibility to respect and protect our privacy rights, but they have instead exploited us for profit. They have made hundreds of billions of dollars at our expense and continue to undermine our fundamental rights. It is time for them to pay the price.

Conclusion

Data and technology companies have grown to wield enormous influence in the Digital Age. They have become some of the most influential and

461. *See supra* Section III.B.

462. *See id.*

powerful companies in human history by engaging in unrestricted surveillance, stockpiling private information, stealing consumers' attention, and selling it for immense profit. The technical infrastructures that these companies have built enable them to follow you across the internet and learn how you think, what you want, and how to influence your behavior, often without your knowledge. They know more about you than your closest friends and use this information however they wish.

These companies use your data to place you into specific categories, decide what content to show you, and target you with custom-tailored advertisements. And the more they learn about your behavior and interests, the better they get. This business model dominates modern society and poses serious concerns for individual autonomy. Through psychological tricks, Big Data manipulates your beliefs and behaviors to make you a more predictable consumer. Additionally, the industry's pervasive data collection and sharing practices undermine your right to privacy at every turn. Collectively, this system prioritizes the profits of corporate giants over the human rights and fundamental freedoms of all.

Fortunately, developments in data privacy law offer encouraging solutions that can empower consumers to reclaim control over their data. By enacting a comprehensive federal data privacy law, Congress can help to restore the balance of power. In doing so, Congress must incorporate best practices that give consumers power over their data, including opt-in consent, straightforward and readable privacy policies, and company transparency. State governments have begun setting aside their political differences to develop creative solutions to what can fairly be considered one of the most important issues of our time. Congress must follow suit before society reaches the point of no return.

Madeline M. Cook