NO MEANS NO: WHY A BRIGHT-LINE RULE AGAINST DATA SHARING IS THE BEST WAY FORWARD FOR PRIVACY LEGISLATION

Erin Husi[*]

TABLE OF CONTENTS

I. INTRODUCTION

In their famous Harvard Law Review article, Warren & Brandeis described the right to privacy as the "right to be let alone."[1] This right has been recognized by the Supreme Court across several areas of the law, including the Fourth

* J.D. Candidate, University of Illinois College of Law Class of 2022. Many thanks to Professor Faye Jones for expert input and generous guidance in writing this Note, and to the editors and members of JLTP for their editing prowess.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

Amendment right against unreasonable search and seizures[2] and the right to privacy in the family.[3] But the "right to be left alone" has not necessarily translated for American individuals in the age of technology, and the United States faces an especially difficult challenge in this area.

Digital personal data receive relatively few legal protections.[4] However, data privacy has gone unregulated in the United States for too long.[5] The question is no longer whether the United States will enact federal privacy legislation. Now, the question is whether a federal privacy bill will effectively address the needs and wants of American consumers concerned about the current state of data collection and their desire for privacy.[6]

To adequately protect consumers from breaches and misuse of data, this Note argues that an effective federal privacy law completely prohibits private entities from sharing user data.[7] This Note will not address use of personal data by public entities, such as in government surveillance. Part II of this Note gives a background on existing privacy law and the problems that have come about as a result of the largely unregulated sharing of user data. Part III analyzes the attitudes of consumers towards privacy and the actions they have taken under other privacy laws in the United States and in Europe. Part IV recommends that, in order to meet the needs of consumers while simultaneously supporting private companies, an American federal privacy law should ban the sharing of data to third parties.

II. BACKGROUND

Understanding privacy law remains a daunting challenge.[8] At times, the term "privacy" has been used to mean several different things: secrecy, surveillance, solitude, transparency, or limited access are just a few examples of privacy's diverse interpretations.[9] Part II provides a general overview of the

2. Katz v. United States, 389 U.S. 347, 350–51 (1967) ("[T]he protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States.").

3. Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965).

4. David Bender & Danice M. Kowalczyk, *Avoiding Intellectual Trespass in the Global Marketplace: Encryption & Privacy in E-Commerce*, 5 VA. J.L. & TECH. 2, 5 (2000) ("Not surprisingly, however, industry self-regulation often falls well short of a comprehensive U.S. privacy protection scheme.").

5. *See* Karen Schuler, *Federal Data Privacy Regulation Is on the Way—That's a Good Thing*, IAPP (Jan. 22, 2021), https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing (discussing the lack of data privacy regulation in the United States).

6. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [hereinafter PEW].

7. As with any good legal rule, there must be some exceptions. Cloud computing, healthcare, and other services may necessitate data sharing. However, this Note considers an outright ban of data sharing to be the most effective floor for an omnibus privacy law.

8. *See generally* Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127 (2006) (providing a detailed background on the different definitions of privacy in law and scholarship).

9. *Id.* at 131–32.

history of privacy in the United States and contextualizes this history as it relates to data privacy in the Internet Age.

A. Privacy Scholarship and Administrative Guidance

Warren & Brandeis's article from over one hundred years ago called for broad protections against privacy intrusions.[10] They imagined a sweeping rule that gave legal protection to an individual's opportunity to control the extent of her thoughts and emotions.[11] Though this idea was directed towards protection from the press,[12] it translates well conceptually to Internet privacy—individuals want to control the extent of their data.[13] Had this formed the basis of existing law, we might be in a different situation today.

However, Warren & Brandeis's broad protections faded in light of a more compartmentalized approach. William Prosser manufactured an understanding of privacy torts that grouped causes of action into four categories: intrusion upon seclusion, public disclosure of private facts, publicity of false information, and appropriation.[14] Prosser obviously shaped the landscape of torts, but his static concepts of four privacy torts have not translated to the protection of informational privacy in the Internet age.[15] In particular, these categories fall short in protecting users from collection and dissemination of data online.[16] As a result, the common law is not currently an effective vehicle in protecting consumers from data sharing among private entities.

As the use of technology became ubiquitous and it became clear that these common law privacy torts would fall short pertaining to the collection of user data, the Federal Trade Commission (FTC) was quick to realize that user information needed to be protected by other means.[17] In 2000, the FTC issued a report to Congress that recognized the benefits of online advertising but also identified that they must be weighed against concerns about the collection of personal data.[18] Some of these concerns included behavioral monitoring without consumers' knowledge, the aggregation of seemingly infinite data to produce profiles that were "inherently intrusive," and discouraging valuable uses of the

10. Warren & Brandeis, *supra* note 1, at 210–11.

11. *Id.* at 198.

12. *See id.* at 196 ("The press is overstepping in every direction the obvious bounds of propriety and decency.").

13. *See infra* Part III. *See generally* PEW, *supra* note 6 (describing consumer attitudes towards privacy).

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

15. Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 90 CALIF. L. REV. 1887, 1922 (2010).

16. *Id.* at 1889.

17. *See* FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS (June 2000), https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf ("Despite the benefits of targeted advertising, there is widespread concern about current profiling practices."); Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899, 907–12 (2011) (describing the FTC's balance of advertising benefits and concern about conducting behavioral profiling without consumer knowledge).

18. Bennett, *supra* note 17, at 907.

Internet based on its perceived anonymity such as sexuality and sexual health information.[19]

Almost a decade later in 2009, the FTC specifically warned against third-party data, or data shared with parties other than the collector, that might be inconsistent with consumer expectations.[20] This required particular attention from the FTC because consumers may not know how to "avoid the practice."[21] Yet again in 2020, a panel of former FTC Commissioners urged Congress to pass federal data privacy legislation.[22] Despite the urgent need for legislative solutions recognized by the FTC for the past twenty years, Congress has chosen not to act.[23] The United States still has no omnibus privacy legislation protecting digital information shared online.[24]

However, there are some federal and state laws that control the dissemination of particular kinds of data. This patchwork approach has made the current state of federal privacy protection a chaotic landscape.[25] For example, federal laws such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule[26] and the Fair Credit Reporting Act (FCRA)[27] protect health information and credit information, respectively. Even still, these laws fall short of expected protections.[28]

For example, there is a wealth of physical and mental health information not protected by HIPAA in the hands of third-party data brokers, including credit card payments for over-the-counter medications, mental health services, home testing products, and free trials of online health services.[29] This is particularly concerning when that information is shared with social media sites like Facebook, which then adds such information to a user's profile.[30]

---

19. *Id.* at 905.

20. *Id.* at 909.

21. *Id.* at 909–10.

22. *Revisiting the Need for Federal Data Privacy Legislation,* SENATE COMM. ON COM. SCI. & TRANSP. (2020), https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation [hereinafter *Data Privacy Hearing*].

23. Bennett, *supra* note 17, at 907.

24. Noah Ramirez, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (Nov. 8, 2020), https://www.osano.com/articles/data-privacy-laws ("There is no one comprehensive federal law that governs data privacy in the United States. There's a complex patchwork of sector-specific and medium-specific laws . . . .").

25. Kenneth A. Bamberger & Dierdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249 (2011).

26. 45 C.F.R. § 164.502 (2021).

27. 15 U.S.C § 1681.

28. Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH 349, 377 (2015) ("The United States has no comprehensive privacy framework, but rather it legislates privacy rights by sector such as with [HIPAA] . . . . This patchwork quilt of privacy protection often leads to uncertainty and confusion among the citizens regarding what rights they may enjoy and under what conditions they may act upon such rights.").

29. Tasha Glenn & Scott Monteith, *Privacy in the Digital World: Medical and Health Data Outside of HIPAA Protections*, CURRENT PSYCHIATRY REP. (2014), https://link.springer.com/article/10.1007/s11920-014-0494-4.

30. Molly Osberg & Dhruv Mehrotra, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020, 1:39 PM), https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (explaining how Facebook obtains access to sensitive mental health data of telehealth users).

Similarly, FCRA was passed in the 1970s when financial information was mostly kept by written records, not digital data.[31] FCRA protects information in credit bureau files but falls short of protecting against incorrect or false demographic or employment information published on third-party websites.[32] Even when data are seemingly protected under FCRA, consumers have an incredibly difficult time correcting errors under the statute.[33] The statute is written for the benefit of credit reporting agencies, who have stretched the "permissible purpose" requirement far beyond any practical limitation.[34] Statutes like FCRA and HIPAA cannot be relied upon as a main vehicle for generally protecting consumer privacy.

B. The Shortcomings of Self-Regulation in the Capitalist Economy

Because of the general lack of adequate federal legislation, companies have done the bare minimum to create an illusion of adequate self-regulation. In the early 2000s, companies created privacy policies that were drafted to inform users of the ways that their information was used and shared.[35] Privacy policies were highly recommended by the FTC to offer clarity on any site's data collection practices and support a framework based on principles of notice and choice.[36] However, a privacy policy simply explains how a company uses data, and the simple existence of one does not guarantee privacy.[37] Furthermore, consumers rarely read through the policy to gain a thorough understanding, and instead interpreted the existence of these policies to mean that their data was protected.[38] Despite these weaknesses, privacy policies continue to be a popular vehicle for companies to convince consumers that their privacy is being protected.[39]

One explanation for this continued reliance on privacy policies could be the influence of the General Data Protection Regulation (GDPR), ratified by the European Union in 2016 and effective January 2018.[40] Though the GDPR protects the privacy of European citizens' data, many companies have looked to it for guidance in their own practices. The GDPR requires privacy policies to be concise and written in plain language.[41] Though this requirement resulted in many companies taking a closer look at their privacy policies,[42] the plain

31. Rachel Bailey, *Consumer Privacy and Legal Risk: What to Look for in the Decade to Come*, CPO MAG. (Feb. 14, 2020), https://www.cpomagazine.com/data-protection/consumer-privacy-and-legal-risk-what-to-look-for-in-the-decade-to-come.

32. *See, e.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330 (2016) (stating respondent did not adequately show injury based on false information purported by Spokeo, Inc. for the purposes of Article III standing).

33. Peek, *supra* note 8, at 135.

34. *Id.*

35. Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 NEW MEDIA & SOC'Y 1824, 1830 (2019).

36. *Id.* at 1831.

37. *Id.*

38. *Id.*

39. *See, e.g.*, TERMAGEDDON, https://termageddon.com (last visited Sept. 28, 2021) (providing custom privacy policies for businesses of all sizes).

40. Commission Regulation 2016/679, 2016 O.J. (L 119) 1.

41. *Id.*

42. DELOITTE, A NEW ERA FOR PRIVACY 7 (2018), https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf.

language requirement sacrificed specificity for generality.[43] What used to be opaque and technical language has become straightforward and easier to read for consumers.[44] But, as previously stated, privacy policies and notices are already crafted to disclose the least amount of detail to consumers.[45] The requirement of plain language is the perfect disguise for the intricacies of data sharing.

Another requirement of the GDPR is an appointment of a "Chief Privacy Officer" (CPO) or "Data Protection Officer" (DPO) within any data processing entity,[46] which many American-based companies have decided to follow.[47] The existence of a CPO or DPO does not necessarily improve privacy practices, but simply ensures the bare minimum of compliance as required by statutes.[48] Internal governance can improve privacy protections within corporations.[49] But when companies choose not only how to protect user privacy but also the person who will serve the interests of shareholders, it creates a conflict of interest.[50] Privacy officers make claims that the ban on data sharing will not protect against abuse yet offer little to no support of that claim.[51] Though the growing popularity—and necessity in the United Kingdom[52] and European Union[53]—of privacy officers is creating some traction in data protection, this role alone will not adequately protect consumers' data in a way that meets consumer expectations and desires.[54]

Some companies have enacted transparency initiatives to gain customers' trust in privacy protocols.[55] But transparency initiatives are often only tools that show how data are being manipulated, and they do not give users increased control over the collection and dissemination of their data.[56] For example, in 2018, data broker Acxiom revealed a program called "About the Data" which provided information for consumers about how their data fueled marketing.[57]

43. *See* Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044, 1081–82 (2017) (explaining the clear language requirement and how it can be abused via generalities instead of specificity).

44. *Id.*

45. Draper & Turow, *supra* note 35, at 1831.

46. Commission Regulation 2016/679, 2016 O.J. (L 119) 1.

47. Bamberger & Mulligan, *supra* note 25, at 261; DELOITTE *supra* note 42, at 10–11.

48. Bamberger & Mulligan, *supra* note 25, at 261.

49. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 50 (2021).

50. *See* Jordan L. Fischer & Michael A. Shapiro, *Beware of Potential Conflicts: Should Your Organization Appoint an IT Director as a Data Protection Officer?*, 3 INT'L DATA PROT. OFFICER, PRIV. OFFICER & PRIV. COUNS. 7, 7–8 (2019) (explaining potential DPO conflicts of interest).

51. *See, e.g.*, Peter M. Lefkowitz, Opinion, *Why America Needs a Thoughtful Federal Privacy Law*, N.Y. TIMES: PRIVACY PROJECT (June 25, 2019) (advancing such a claim with little evidentiary support), https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html.

52. *See Data Protection Officers*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers (last visited Sept. 28, 2021) ("The UK GDPR introduces a duty for you to appoint a data privacy officer.").

53. *What Is a GDPR Officer and Who Needs to Appoint One?*, GDPR EU, https://www.gdpreu.org/the-regulation/key-concepts/data-protection-officer (last visited Sept. 28, 2021) ("GDPR legislation says that Data Protection Officers (DPO) must be appointed by some companies.").

54. *See* Bamberger & Mulligan, *supra* note 25, at 301–02 (recounting consumer expectations of privacy and how procedural safeguards fell short with Intel Pentium chips).

55. *Id.* at 266.

56. *Id.* at 301–02.

57. Matthew Crain, *The Limits of Transparency: Data Brokers and Commodification*, 20 NEW MEDIA & SOC'Y 88, 92–93 (2018).

However, Acxiom only disclosed a small portion of the vast amounts of data that it retained on consumers and explained very little on the source or destination of such data points.[58] What was supposed to be a data transparency initiative did not offer any option for consumers to control, delete, or otherwise manage the data retained by third parties.[59]

In addition to the Acxiom tool, Facebook has tried to mitigate concerns of data sharing through similar initiatives. After the Cambridge Analytica scandal,[60] Facebook sent users to a site where they could discover much of the information stored about them.[61] Despite Facebook's attempt at transparency, users found that they could not delete data that they found objectionable or in violation of their personal privacy concerns.[62] These examples suggest that Facebook's promise of self-regulation simply was "part of an obfuscation process that often uses the rhetoric of placation and diversion."[63] Private entities are testing the waters with the least possible interruptions to their data sharing practices in order to protect themselves and prevent substantive reforms in the way data are shared.[64] In sum, transparency initiatives are more words than actions—they do not actually offer anything in the way of increased protections of consumer information stored online by companies.

Although companies tout the importance of sharing data,[65] often the complexity of data processing surpasses any one individual's (or company's) understanding of data manipulation and conglomeration.[66] Despite benefitting from data collection and manipulation, companies do not have a thorough understanding of the way they use data.[67] Without this understanding, companies can hardly be expected to be able to communicate to customers every way in which data are used, and the ways are unbelievable.

---

58. *Id.*

59. *Id.* at 95.

60. Nicolas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

61. Draper & Turow, *supra* note 35, at 1832.

62. Brian X. Chen, *I Downloaded the Information that Facebook Has on Me. Yikes.*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/personaltech/i-downloaded-the-information-that-facebook-has-on-me-yikes.html.

63. Draper & Turow, *supra* note 35, at 1832.

64. *Id*.

65. Issie Lapowsky, *How Tim Cook's Data Broker Registry Might Actually Work*, WIRED (Jan. 23, 2019, 12:25 PM), https://www.wired.com/story/tim-cook-data-broker-registry.

66. *See* Louis Menand, *Why Do We Care So Much About Privacy?*, NEW YORKER (June 18, 2018) ("[W]e don't really know who is seeing our data or how they're using it. Even the people whose business it is to know don't know"); Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 96 (2014) ("Users have been unaware of the breadth and depth of the market for personal information. Even industry veterans struggle to explain the intricacies of the data flows").

67. *See* Cynthia Johnson, *How Data Complexity Is Changing the Face of Business Analytics*, FORBES (Nov. 3, 2016), https://www.forbes.com/sites/forbesagencycouncil/2016/11/03/how-data-complexity-is-changing-the-face-of-business-analytics/ ("[A]s the data gets bigger and more prominent, executives start to expect line-of-business (non-technical) managers to be able to understand and present insights extracted from complex, distinct and often unstructured datasets . . . prompting a decline in the quality of data being used by businesses to make decisions.").

Despite decades of the FTC urging Congress to act,[68] a federal privacy law has yet to be passed in the United States, and it is clear that neither existing legislation nor self-regulation are viable options for protecting consumer data.[69] Part III explores the views and goals of both consumers and businesses to help inform the structure and main components of a federal privacy law.

III. ANALYSIS

The lack of data protection that consumers currently face in the marketplace has exposed the failures of self-regulation. A federal privacy law is necessary to adequately protect consumer data. This analysis explores the risks of inadequate protections, the consumer views and actions under existing legislature that should inform federal privacy legislation, and the proposals and shortcomings of non-governmental solutions to the problems of data privacy.

A. The Consequences of the Lack of Privacy Protections

1. Data Breaches

The most obvious and expensive problem with data sharing is the increased risk of data breaches which expose consumers' private information.[70] This is a problem facing both companies and consumers. In 2019, data breaches cost U.S. companies $8.19 million on average.[71] While companies are hit hard in settlements, consumers rarely see significant relief whether financially or in the form of increased protection. Remedies for individuals are usually low sums that hardly compensate for the long-term effects of data breaches, or some form of reimbursement for identity theft protection services or discounts on previously purchased subscriptions.[72] Though data breaches can be remedied under existing law,[73] the prevalence of these breaches exposes the dangers of continuing unmonitored data sharing, particularly for the consumer. Without a thorough understanding of how many and which companies have data, and what kind of data they may possess, it is impossible for Internet users to fully protect themselves against a data breach.

However, data breaches affect more than consumers' pocketbooks. In 2016, Cambridge Analytica harvested private information from upwards of fifty

68. Bennett, *supra* note 17, at 906.

69. *Id*.

70. Chris Brook, *What's the Cost of a Data Breach in 2019?*, DIGITAL GUARDIAN (Dec. 1, 2020), https://digitalguardian.com/blog/whats-cost-data-breach-2019.

71. *Id*.

72. Tony Larussa, *How to Get Your Share of $700M Settlement from Equifax Data Breach*, PITT. TRIB. REV. (July 25, 2019, 9:45 AM), https://triblive.com/local/regional/people-affected-by-2017-equifax-data-breach-can-apply-online-for-share-of-settlement/; *Yahoo Is Compensating Victims of Their Massive Data Breach*, I.T. SOLUTIONS, https://www.itsolutions247.com/blog/yahoo-is-compensating-victims-of-their-massive-data-breach/ (last visited Feb. 6, 2020).

73. *Id*.

million Facebook users without their permission.[74] This information was used by the 2016 and 2020 Trump campaigns—even after questions arose surrounding the ethical and legal nature of Cambridge Analytica's activities in 2014—to design target audiences for digital ads and fundraising, modeling voter turnout, and determining campaign locations.[75] Cambridge Analytica's CEO claimed that these practices had a significant influence on the 2016 election.[76] Additionally, Facebook was the main source of misinformation regarding the 2020 election.[77] Misinformation, Facebook admits, is largely based on data collected from the vast amounts of user data this social media company holds.[78] The lack of federal data privacy legislation leaves open the possibility that national or international actors may threaten democracy by using data that are traded and shared without user knowledge or consent.

2. Social Norm Nudges

Although Facebook claimed that data were improperly collected in the Cambridge Analytica scandal,[79] Facebook has continued to make unpopular decisions about sharing user data.[80] In 2018, data-sharing arrangements between the social media giant and Spotify, Amazon, and Netflix (among others) were revealed, and the public learned that these companies had access to personal data far beyond what had been previously disclosed.[81] In 2021, WhatsApp (a Facebook company) released a new privacy policy that prompted massive outrage against the app collecting activity logs, device and connection logs, location data, and interactions with business accounts.[82] As a result, even more data on users has likely been accumulated by countless data brokers.[83]

The more data is accumulated and shared, the more pressing these privacy concerns become as almost any behavior can be motivated by data manipulation.

---

74. Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

75. *Id.*

76. Eric Auchard & David Ingram, *Cambridge Analytica CEO Claims Influence on U.S. Election, Facebook Questioned*, REUTERS (Mar. 20, 2018), https://www.reuters.com/article/us-facebook-cambridge-analytica/cambridge-analytica-ceo-claims-influence-on-u-s-election-facebook-questioned-idUSKBN1GW1SG.

77. Isabelle Lee & Sarah Frier, *Most US Voters See Misinformation Online and Many Believe It*, BLOOMBERG (Oct. 26, 2020, 9:16 AM), https://www.bloomberg.com/news/articles/2020-10-26/most-u-s-voters-see-misinformation-online-and-many-believe-it.

78. *See generally* Nick Statt, *Facebook Will Let Researchers Study How Advertisers Targeted Users with Political Ads Prior to Election Day*, VERGE (Jan. 25, 2021, 1:36 PM), https://www.theverge.com/2021/1/25/22248806/facebook-us-2020-election-data-research-political-ad-targeting (stating that Facebook's user data has been utilized to target certain demographics).

79. John Constine, *Cambridge Analytica Denies Accessing Data on 87M Facebook Users…Claims 30M*, TECHCRUNCH (Apr. 4, 2018, 5:39 PM), https://techcrunch.com/2018/04/04/cambridge-analytica-30-million/.

80. Alexis Madrigal, *Facebook Didn't Sell Your Data; It Gave It Away*, ATLANTIC (Dec. 19, 2018), https://www.theatlantic.com/technology/archive/2018/12/facebooks-failures-and-also-its-problems-leaking-data/578599.

81. *Id.*

82. Daniel Cooper, *WhatsApp Reassures Users It Can't Read Their Messages*, ENGADGET (Jan. 12, 2021), https://www.engadget.com/whatsapp-privacy-policy-changes-statement-encryption-surveillance-172224753.html.

83. Lily Hay Newman, *WhatsApp Has Shared Your Data with Facebook for Years, Actually*, WIRED (Jan. 8, 2021, 1:52 PM), https://www.wired.com/story/whatsapp-facebook-data-share-notification.

"Social norm nudges," or widespread inducement of particular decisions, can influence decisions from which clothes to buy to whom to vote for in elections.[84] Nudges are informed not only by the type of data-sharing mentioned above, but also by social media practices such as "social listening." Social listening is the process of analyzing social media pages to create a robust profile of the user as a consumer.[85] Though many sites consider social listening a legitimate business practice,[86] the uses of this privacy intrusion are shocking. For example, social listening can be used for determining credit risks and setting loan interest rates.[87] Invasive collection and sharing tactics are said to support local or small businesses and their ability to provide marketing;[88] however, some experts believe that the efficacy of Internet marketing is a wholly unexplored idea, and the bubble will soon pop.[89] The benefits of social listening and online advertising may not be worth it when compared to the cost of data breaches, weakening democracy, and widespread concern about manipulating behavior.[90]

Anna Wiener, in her memoir *Uncanny Valley*, details the specificity in which data can be used to find and influence users:

> Data could be segmented by anything an app collected—age, gender, political affiliation, hair color, dietary restrictions, body weight, income bracket, favorite movies, education, kinks, proclivities—plus some IP-based defaults, like country, city, cell phone carrier, device type, and a unique identification code. If women in Boise were using an exercise app primarily between the hours of nine and eleven in the morning—only once a month, mostly on Sunday, and for an average of twenty-nine minutes—the software could know . . . . All customers had to do was run a report; all they had to do was ask.[91]

3. Data and Civil Rights

Beyond feelings of general creepiness and upset at this war between seemingly powerless consumers and manipulative organizations, there is a civil rights crisis underlying issues of data privacy. Privacy issues are exacerbated in low-income communities, having a disparate effect on communities of color.[92]

---

84. *See generally* Yifat Nahmais et al., *Privacy Preserving Social Norm Nudges*, 26 MICH. TECH. L. REV. 43 (2019) (explaining the possibilities and implications of social norm nudges).

85. Tene & Polonetsky, *supra* note 66, at 62.

86. *See* Swetha Amaresan, *What Is Social Listening and Why Is It Important?*, HUBSPOT BLOG, https://blog.hubspot.com/service/social-listening (last visited Feb. 6, 2020) (suggesting that businesses integrate social listening as part of their marketing strategy).

87. Tene & Polonetsky, *supra* note 66, at 62.

88. Bart de Langhe & Stefano Puntoni, *Facebook's Misleading Campaign Against Apple's Privacy Policy*, HARV. BUS. REV. (Feb. 2, 2021), https://hbr.org/2021/02/facebooks-misleading-campaign-against-apples-privacy-policy.

89. Gray Area, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*, YOUTUBE (Oct. 12, 2020), https://www.youtube.com/watch?v=X9dlJ4sHfSk [hereinafter Subprime Attention Crisis].

90. *Id*.

91. ANNA WIENER, UNCANNY VALLEY: A MEMOIR 43 (MCD 2020).

92. PEW, *supra* note 6. For an exploration of the harms of extreme privacy, see Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. &

For example, Black adults are roughly three times as likely as white or Hispanic counterparts to say someone has taken over their social media account or email address in the past year.[93] Black adults are also more likely to report credit fraud.[94] Beyond race-based discrimination, privacy violations exploit gender norms, economic disparity, and agism: low-income individuals are targeted for predatory marketing campaigns,[95] women are excluded from job opportunities,[96] and young students visiting college websites are targeted for massive, high-interest loans.[97]

Disparity appears even at the hardware level. Android devices, made by Google, do not encrypt data stored on the device by default, nor did Android's text messaging app use encryption as of 2020.[98] By contrast, Apple markets to wealthy customers by offering device security and encryption.[99] Apple even uses privacy as a marketing tool, making broad claims of valuing privacy without exposing particulars.[100] As a result, the personal information of wealthy, predominantly white customers is protected, while those in vulnerable communities do not have access to such protection.[101]

Clearly there are significant risks to maintaining the status quo of unbridled data collection. Though consumers may not be aware of all these risks, one can glean a significant amount of information about the types of protection they might seek from survey attitudes and actions taken under existing privacy statutes that may inform a blueprint for a federal privacy law.

B. Learning from American Consumers

1. Consumer Opinions

Despite severe political turmoil,[102] bipartisan support for privacy legislation in the United States evinces the urgent need for a broad federal privacy law. In 2019, 79% of voters believed Congress should prioritize crafting a bill to protect user privacy.[103] This number includes 83% of Democrats and

SOC. CHANGE 253, 254–55 (2018) ("[M]arginalized people experience privacy differently than most Americans. Specifically, they experience privacy extremes . . . .").

93. PEW, *supra* note 6.

94. *Id.* (showing 12% of Black adults reporting credit fraud compared to 7% of Hispanic adults and 4% of white adults).

95. Michele E. Gilman, *Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice*, 52 ARIZ. ST. L.J. 368, 371 (2020).

96. *Id.* at 379.

97. *Id.* at 382.

98. Christopher Soghoian, *Your Smartphone Is a Civil Rights Issue*, TED (June 2016), https://www.ted.com/talks/christopher_soghoian_your_smartphone_is_a_civil_rights_issue/transcript.

99. *Id.*

100. *See, e.g.*, Apple, *Privacy. That's iPhone. – Over Sharing*, YOUTUBE (Sept. 3, 2020), https://www.youtube.com/watch?v=-l61NE0eqkw.

101. *Id.*

102. Lauren Leatherby et al., *How a Presidential Rally Turned into a Capitol Rampage*, N.Y. TIMES (Jan. 12, 2021), https://www.nytimes.com/interactive/2021/01/12/us/capitol-mob-timeline.html.

103. Sam Sabin, *Most Voters Say Congress Should Make Privacy Legislation a Priority Next Year*, MORNING CONSULT (Dec. 18, 2019, 12:01 AM), https://morningconsult.com/2019/12/18/most-voters-say-congress-should-make-privacy-legislation-a-priority-next-year.

82% of Republicans.[104] Although privacy may not be at the top of the Biden administration's agenda,[105] the crucial timing of this overlap in political support should not be ignored.

American consumers have not been ignorant to the increasingly concerning implications of a lack of data privacy—current attitudes are characterized by awareness and concern.[106] In 2019, 79% of Americans were concerned about the way that companies use their data.[107] More specifically, 81% of American consumers understand that they have little or no control over the amount of data companies collect from them.[108] The same percentage believe that the risks of private companies collecting private data do not outweigh the benefits.[109]

This concern may be motivated by a lack of understanding: 60% of respondents had little to no understanding of how data collected by companies are used.[110] Though consumers may not understand how data are collected, they are obviously concerned about the immediate and long-term implications of the current collection and sharing practices.[111]

Americans believe that they are unprotected by legislation.[112] 69% of consumers said they are not confident that companies use data in ways with which users are comfortable, and 75% are not confident that companies would be held accountable by the government if companies misuse consumer data.[113] These numbers suggest the need for protection on a federal level comes down to a balance of power: consumers do not know how companies use their data, they do not trust companies to use it in ethical ways, and they do not believe that there will be accountability when data use crosses a line.[114] This lack of accountability and trust must be remedied by a federal privacy law.

This power imbalance can be characterized by the concept of "privacy resignation," or reconciling a desire to control the information digital entities have with an overwhelming feeling of the inability to do so.[115] In a 2015 survey, 58% of respondents showed resignation based on their agreement with two statements: "I want control over what marketers can learn about me online" and "I've come to accept that I have little control over what marketers can learn about me online."[116] Although a majority of Americans are aware of the ways in which companies collect their data and express a desire to have more control

104. *Id.*

105. *See* Alana Abramson & Brian Bennett, *Inside Joe Biden's Agenda for His First 100 Days*, TIME (Jan. 21, 2021), https://time.com/5931852/joe-biden-100-days/ (mentioning no attempts to address digital privacy in President Biden's first 100 days).

106. PEW, *supra* note 6.

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.*

114. *Id.*

115. Draper & Turow, *supra* note 35, at 1824; JOSEPH TUROW, MICHAEL HENNESSY & NORA DRAPER, THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 3 (2015) [hereinafter TRADEOFF FALLACY].

116. Draper & Turow, *supra* note 35, at 1824.

over the spread of that data, they also carry a pervasive sense of hopelessness that they ultimately will never have any control over it.[117]

This resignation explains the privacy paradox, or the cognitive dissonance between attitudes towards privacy and actions to protect privacy.[118] For example, American consumers who are concerned with the protection of their privacy are not often likely to engage in privacy-protective behaviors, even engaging in risky behaviors such as voluntarily disclosing critical personal information on social media sites.[119] While some argue that this type of behavior signals that consumers do not actually care about privacy and regulations should be lessened,[120] it is more helpful to think about this "paradox" as informative for the way legislation should move forward.[121]

The privacy paradox is less of an indication that consumers do not actually care about privacy and more a product of a lack of options that do not involve significant technical literacy. The privacy paradox is buttressed by privacy protection models of self-management, as encompassed by existing legislation such as the California Consumer Privacy Act and the right to opt out.[122] But this approach to privacy management and data control presupposes a knowledge of the types of and ways in which data are collected.[123] Daniel Solove compares privacy self-management, such as consent boxes and cookie switches, to "doling out yet more homework, heaping on more tasks that people lack the time or ability to do."[124] An overall privacy protection strategy that is fully based on self-management will not be fully adequate to address these concerns.

Interestingly, there is one area in which Americans have voiced significant aversion to sharing data. During the COVID-19 crisis, public attitudes toward contact tracing apps have been generally negative—people do not trust companies to use their data.[125] In a survey taken June of 2020, 71% of respondents would not use contact tracing apps, primarily out of concern for their personal privacy and a lack of trust in companies like Apple and Google.[126] But contact tracing was essential in containing the virus in other countries that returned to "normal" much faster than the United States.[127] With better tools to protect individual privacy, a widespread aversion to contact tracing may not have been such a significant issue in containing the spread of COVID-19 in 2020 and may have led to a better balance of protecting public health and

117. *Id.*
118. *Id.* at 1825.
119. Young Min Baek, *Solving the Privacy Paradox: A Counter-Argument Experimental Approach*, 38 COMPUT. HUM. BEHAV. 33, 34 (June 11, 2014).
120. Solove, *supra* note 49, at 11.
121. *Id.* at 33.
122. *Id.* at 30 n.151, 46.
123. *Id.* at 46.
124. *Id.* at 49.
125. Jessica Rich, *How Our Outdated Privacy Laws Doomed Contact-Tracing Apps*, BROOKINGS (Jan. 28, 2021), https://www.brookings.edu/blog/techtank/2021/01/28/how-our-outdated-privacy-laws-doomed-contact-tracing-apps.
126. *Id.*
127. *See generally* April Xiaoyi Xu, *But What If Big Brother Saves Lives? Comparative Digital Privacy in the Time of Coronavirus*, 54 CREIGHTON L. REV. 147 (2020) (laying out a thorough investigation on global contact tracing effort and the effect of COVID-19 on privacy).

quarantining.[128] Had Congress acted sooner, the COVID-19 experience in the United States could have gone very differently.

2. Consumer Actions Under Existing Privacy Legislation

Despite its shortcomings, the California Consumer Privacy Act (CCPA) has been an interesting experiment in scalable privacy legislation. Consumers' actions under the CCPA seem to match the concerns evinced by their attitudes: by the seven-month mark after the CCPA went into effect, fifty lawsuits had been filed citing the CCPA as grounds for recovery, several of which were class actions.[129] However, as the CCPA only allows a private right of action when personal information has been shared as result of a breach, this litigation does not necessarily protect forward-looking privacy concerns.[130]

For example, in *Guzman v. RLI Corp.*, the plaintiffs were denied an injunction to prevent the defendant from disclosing sensitive immigration information because, according to the court, there was "no emergency shown as to the general claim that there is an immediate, material risk that Defendants will disclose confidential information about the Plaintiff or putative class members in some other manner."[131] In contrast, *Stasi v. Inmediata Health Group* survived a motion to dismiss under the CCPA because the plaintiffs' information "was viewed by unauthorized persons."[132] *Stasi* also suggests that plaintiffs need not prove theft or unauthorized access to plead a plausible violation of the CCPA, yet this lack of proof seemed to bar the claims in *Guzman.*[133] There are several pending suits citing the CCPA as grounds for remedy, many of which include allegations of using or sharing personally identifiable information without providing required notice.[134]

Though the CCPA is the broadest existing piece of privacy legislation among the states,[135] there are other pieces of legislation that protect particular types of digital privacy that can inform a federal privacy law blueprint. For example, Illinois passed the Biometric Information Privacy Act (BIPA) in 2008, an act that regulated the use of biometric data.[136] Specifically, biometric data refers to "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face

128. *Id.*

129. Mark S. Melodia, Ashley L. Shively & Mark H. Francis, *Litigating the CCPA in Court*, HOLLAND & KNIGHT ALERT (July 22, 2020), https://www.hklaw.com/en/insights/publications/2020/07/litigating-the-ccpa-in-court.

130. *Id.*

131. Guzman v. RLI Corp., No. LA CV20-08318 JAK (ASx), 2020 WL 6815026, at *2 (C.D. Cal. Oct. 6, 2020).

132. Stasi v. Inmediata Health Grp. Corp., No. 19CV2353 JM (LL), 2020 WL 6799437, at *909 (S.D. Cal. Nov. 19, 2020).

133. *See id.* at *924 ("Moreover, Inmediata does not point to any authority requiring Plaintiffs to plead theft or unauthorized access in order to plead a plausible violation of the CCPA."); *cf. Guzman*, 2020 WL 6815026, at *2 ("Based on the present record, Plaintiff has not shown the need for emergency injunctive relief to prevent immediate and irreparable harm.").

134. *See, e.g.*, Taylor v. Zoom, No. 5:20-cv-02170 (N.D. Cal. filed Mar. 31, 2020); Rios v. Zoom, No. 5:20-cv-03670 (N.D. Cal. filed June 2, 2020).

135. Stuart D. Levi & James S. Talbot, *California Enacts Sweeping New Privacy Law*, SKADDEN (July 11, 2018), https://www.skadden.com/insights/publications/2018/07/california-enacts-sweeping-new-privacy-law.

136. 740 ILL. COMP. STAT. 14/1.

geometry."[137] BIPA has resulted in hefty penalties against noncompliant companies, with the biggest recovery to date in the form of a settlement for $650 million against Facebook for its facial recognition technology used in the "tag suggestions" feature.[138] In addition to providing payouts of $200–$400 per class member,[139] Judge Donato allowed the case to settle because of Facebook's remedial measure of globally changing its facial recognition to an opt-in default setting.[140] Although BIPA only applies to biometric privacy, expensive settlements like the one with Facebook, as well as BIPA's ongoing popularity with the plaintiffs' bar, suggest that social media giants will no longer go completely unchecked as they continue to exploit user data.

Though not necessarily a direct protection for consumers, Vermont passed a "data broker" registry law in 2018.[141] This law requires data brokers, or business units that "knowingly collect[] and sell[] or license[] to third parties the brokered personal information of a consumer with whom the business[es] do[] not have a direct relationship,"[142] to register with the state.[143] While the law requires these businesses to identify whether or not consumers can opt out, it does not require data brokers to give consumers the option to opt out or delete their data.[144] This law is not simply on the books—Vermont's Attorney General filed a suit against Clearview AI in 2020 for violating the statute.[145] While a registry is one step in illuminating an opaque industry of data sharing, it is still unclear whether consumers will embrace this method.

Outside of the United States, there is another piece of significant legislation that must be considered as another case study in consumer actions under privacy law. In 2016, the EU adopted the General Data Protection Regulation (GDPR) which went into effect in 2018.[146] This sweeping legislation changed the privacy landscape overnight and resulted in an endless pinging of email inboxes full of new, updated privacy policies.[147] Three years later, it continues to shed light on the disparity of protections between EU and U.S. consumers. The GDPR contains core rights for EU consumers that most U.S. consumers do not yet enjoy—except Californians who enjoy certain rights under the CCPA.[148] Notably, these rights include the right to be informed of when and how data are

137. 740 ILL. COMP. STAT. 14/10.

138. Blank Rome, *Impact of Facebook $650 Million Patel BIPA Settlement*, BIOMETRIC UPDATE (Aug. 20, 2020), https://www.biometricupdate.com/202008/impact-of-facebook-650-million-patel-bipa-settlement.

139. FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION, http://www.facebookbipaclassaction.com (last visited Sept. 27, 2020).

140. Rome, *supra* note 138.

141. Steven Melendez, *A Landmark Vermont Law Nudges Over 120 Data Brokers Out of the Shadows*, FAST COMPANY (Mar. 2, 2019), https://www.fastcompany.com/90302036/over-120-data-brokers-inch-out-of-the-shadows-under-landmark-vermont-law.

142. 9 V.S.A. § 2430(4).

143. Melendez, *supra* note 141.

144. *Id.*

145. Divonne Smoyer, Samuel F. Cullari & Alexis Cocco, *Vermont Attorney General Brings First Data Broker Enforcement Action*, REED SMITH TECH. L. DISPATCH (Mar. 17, 2020), https://www.technologylawdispatch.com/2020/03/privacy-data-protection/vermont-attorney-general-brings-first-data-broker-enforcement-action.

146. Commission Regulation 2016/679, 2016 O.J. (L 119) 1.

147. *See id.* (requiring increased clarity of a privacy policy).

148. Gilman, *supra* note 95, at 413, 442.

being collected and processed, the right to withdraw consent to processing of personal data, and the right to be "forgotten" or to have personal data erased.[149]

The GDPR opened the floodgates for litigation in the EU.[150] The most notable of which is the famous Max Schrems suit against Facebook (one suit in a string of battles) accusing Facebook of coercing users into accepting their data privacy practices, filed just hours after the GDPR was passed.[151] Schrems' non-profit organization, "noyb" (which stands for none of your business) zealously advocates for consumer rights under the GDPR.[152] Several other class actions have been filed in Europe in the post-Schrems litigation swell, with damages totaling in the millions against large companies such as Google and Facebook.[153] As litigation continues, the evolution of the GDPR will likely be a balancing act between consumer and corporate interests.

While American attitudes towards data privacy indicate a thus far failure of U.S. government to address issues of privacy, EU citizens' attitudes towards the GDPR illustrate its strengths and weaknesses. Despite non-profits like noyb, the general attitudes on an individual level toward the GDPR vary. In a Deloitte survey, 21–29% of EU users had no intention of exercising their rights under the GDPR, while up to 40% of respondents have either already taken advantage of the right or may use it in the future (percentages varying depending on the right).[154] Willingness to share information depends on the type of data as well: users are more willing to share information on consumption habits than health or wealth information.[155] These numbers may change as more individuals are educated on their rights—only about 80% of respondents were aware of the rights granted under the GDPR.[156] As time goes on and technical literacy increases across the board, more individuals may decide to opt out and take advantage of the rights awarded to them under the GDPR.

Presently, the biggest difference between the EU and the U.S. privacy laws is one of concept. Europeans consider privacy a human right that constrains both governments and private entities.[157] Though Americans seem to agree,[158] American governance has not yet embraced this through legislative solutions.[159]

149. *Id.* at 414.

150. Angelique Carson, *GDPR Ushers in Civil Litigation Claims Across the EU*, IAPP (Mar. 24, 2020), https://iapp.org/news/a/gdpr-ushers-in-civil-litigation-claims-across-the-eu.

151. Derek Scally, *Max Schrems Files First Case Under GDPR Against Facebook and Google*, IRISH TIMES (May 25, 2018, 6:15 AM), https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177.

152. *Id.*

153. *GDPR Fines and Penalties*, NATHAN TRUST, https://www.nathantrust.com/gdpr-fines-penalties (last visited Sept. 25, 2021).

154. DELOITTE, A NEW ERA FOR PRIVACY (2018), https://www2.deloitte.com/au/en/pages/risk/articles/new-era-privacy.html.

155. M. Karampela et al., *Exploring Users' Willingness to Share Their Health and Personal Data Under the Prism of the New GDPR: Implications in Healthcare*, *in* 41ST ANN. INT'L CONF. IEEE ENG'G MED. & BIOLOGY SOC'Y 6509–6512 (July 2019), https://ieeexplore.ieee.org/abstract/document/8856550.

156. *Id.*

157. Gilman, *supra* note 95, at 413.

158. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNS. ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

159. *Id.*

Despite the existence of private solutions, Congress has still fallen short in terms of protecting consumer interests.[160]

C. Non-Legislative Technological Solutions and Their Shortcomings

Though other solutions have been proposed to meet consumer desires for increased data protection, they have proven unsuccessful. Self-regulation has failed as a policy, and even if the suggestions below were to be legislated, they would still fall short.[161] Improved security of data still does not solve the problem of data autonomy.[162] Additionally, if proposed solutions put the onus of change on corporations, they will continue to act in their own self-interest, maintaining the existing regime of the shortcomings of self-regulation.[163]

One solution that has been proposed for creating adequate privacy protection through legislation is the requirement of "opt-in" over "opt-out" models of data sharing and consent.[164] Certain privacy scholars see opt-in models as a way to honor an individual's choice to avoid being subject to unconsented-to data sharing.[165] But toggling opt-in and opt-out buttons is simply another tool with which companies create the illusion of control.[166] The Internet should not become a series of obstacles that consumers are expected to research and choose before getting to the content they originally sought out from a supposedly swift and effective search engine. Creating more work for consumers is not the best way to address data privacy.

Other privacy advocates argue that individuals lack the necessary knowledge to make informed decisions on the consequences of opting into a marketing transaction.[167] In addition, users typically click through agreements without thoroughly reading them, frustrated by uninvited or unexpected interruptions to browsing activity.[168] This "solution" is hardly a solution at all, and it certainly does not solve the problem of comprehensiveness in data management processes.[169] It simply adds one more annoying button to click and assumes a level of technical literacy that not all consumers possess.

An opt-in model would also invite increased costs for small businesses who lack the capital and know-how to comply and might ultimately favor large

---

160. *Id.*

161. Katitza Rodriguez, *Data Protection Regulation and the Politics of Inoperability*, ELEC. FRONTIER FOUND. (Dec. 22, 2011), https://www.eff.org/deeplinks/2011/12/data-protection-regulation-and-politics-interoperability.

162. *See Data Privacy vs Data Security [Definitions and Comparisons]*, DATA PRIV. MANAGER (Oct. 1, 2021), https://dataprivacymanager.net/security-vs-privacy (noting that data privacy and security are entirely different concepts and require different protections).

163. *See* ANA ISABEL SEGOVIA DOMINGO & NATHALIE DESMET VILLAR, SELF-REGULATION IN DATA PROTECTION 2 (2018) (explaining that self-regulation by companies is not working satisfactorily in the United States).

164. Joseph A. Tomain, *Online Privacy and the First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV. 1, 11 (2014).

165. *Id.*

166. Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 811 (2020).

167. TRADEOFF FALLACY, *supra* note 115, at 7.

168. Tene & Polonetsky, *supra* note 66, at 75.

169. *Id.*

companies who have the bandwidth to comply.[170] The CCPA recognizes this, and only requires businesses of certain sizes to comply.[171] However, when small businesses do not comply, they continue to put consumers at risk.[172] Privacy legislation should address the capabilities of both small and large companies, and should enable businesses of all sizes to protect consumer data.

Another proposed solution is the use of anonymization techniques that allow organizations to process an individual's information without sacrificing privacy.[173] However, this approach does not solve the issue of transparency, and ultimately does not protect an individual's privacy at all.[174] For example, Netflix's anonymization techniques were quickly de-anonymized by researchers at the University of Texas, which ultimately resulted in a lawsuit against the company for a violation of the Federal Video Privacy Protection Act.[175]

Consider device-fingerprinting as well: even when consumers have the option to opt out of tracking, other identifiers can give a person's identity away.[176] Because of the advanced technology available, de-identification techniques make even anonymized data vulnerable.[177] In the words of one reporter, "arguing that a customer record is 'anonymous' and thus does not constitute 'selling' data merely because it uses an IP address instead of a phone number as an identifier is simply an absolute falsehood in today's data drenched world."[178] Aggregation simply creates another minimal obstacle that is sure to be easily overcome by anyone who wants access to consumer data.

Differential privacy—a mathematical framework that adds uncertainty to data analysis—has been proposed as a solution to the weaknesses of anonymization techniques.[179] This solution is insufficient for several reasons. First, it still does not fix the problem of transparency for consumers. Adding more confusion to the way data are processed does not solve the problem of a lack of control over the way data are used and processed.[180] Second, the cost of such advanced computing programs may not be attainable for small businesses

170. Will Rinehart, *Opt-In Mandates Shouldn't Be Included in Privacy Laws*, AM. ACTION F. (Nov. 8, 2018), https://www.americanactionforum.org/insight/opt-in-mandates-shouldnt-be-included-in-privacy-laws.

171. *CCPA Compliance Guide*, VARONIS (June 17, 2020), https://www.varonis.com/blog/california-consumer-privacy-act-ccpa.

172. *See generally* Tomain, *supra* note 164 (explaining that compliance with opt-in provisions would protect consumer liberties and rights).

173. Nahmias, *supra* note 84, at 76.

174. *Anonymization*, IMPERVA, https://www.imperva.com/learn/data-security/anonymization (last visited Sept. 27, 2021).

175. *Id*.

176. *Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE @ WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done.

177. *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 37 (2010), http://www.ftc.gov/os/2010/12/ 101201privacyreport.pdf ("[E]ven where companies take steps to 'de-identify' data, technological advances and the widespread availability of publicly available information have fundamentally changed the notion of anonymity.").

178. Kalev Leetaru, *What Does It Mean for Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/.

179. Nahmias, *supra* note 84, at 79.

180. *See* WEAKNESSES OF DIFFERENTIAL PRIVACY, COURSERA, https://www.coursera.org/lecture/data-results/weaknesses-of-differential-privacy-50Y9k (last visited Sept. 25, 2021) (explaining the complexities of differential privacy).

and would favor large organizations with more capital.[181] Finally, it would further confuse lawyers and judges on interpreting privacy law.[182] Evaluating advanced statistical models under a privacy law would almost certainly yield more confusing opinions and interpretations than clear ones.

Based on the shortcomings of these proposed solutions, and the weaknesses of existing legislation, it is time to think outside the box. There is a simple solution to this problem that has not been fully considered yet: stop companies from sharing consumer data altogether. Part IV discusses the viability of this option as the best avenue forward for protecting consumer data and recognizing the capabilities of businesses of all sizes across the nation.

IV. RECOMMENDATION

The status quo of self-regulation is no longer acceptable practice, and a federal privacy law is paramount to protecting consumers' data. Consumers have made their position clear: they want their privacy to be protected, and if given the opportunity, they are enforcing the rights granted by privacy legislation. The best and most practical way to do this is through legislation that completely prevents the sharing of data by private entities. Part IV explains why a bright-line rule against sharing data provides the best model for a federal privacy law.

A. The Best Way Forward for Consumers

Consumers want more control over their data, and when third parties are involved, such control becomes almost impossible.[183] If third parties were taken completely out of the equation, it would afford consumers a much better ability to understand who has what data about them.[184] Therefore, consumers would have full control over the extent to which they decide to share data as well as a confidence in the purpose limitations for which the data would be used as described by the company.[185] Data broker laws, compliance requirements, and other obstacles currently being debated would no longer be necessary.[186]

This practice should take the form of a federal law instead of a patchwork of state laws because consumers deserve equal protection across states. This would also simplify potential questions of state law protections: are you protected from the location of your IP address, or permanent mailing address? If

181. *See* Syed Atif Moqurrab, Comment to *I Would Like to Know the Limitations or Weaknesses of Differential Privacy in Preserving Privacy in Deep Learning?*, RESEARCHGATE (Feb. 26, 2020), https://www.researchgate.net/post/I-will-like-to-know-the-limitations-or-weaknesses-of-Differential-Privacy-in-preserving-privacy-in-deep-learning ("It is computationally very expensive.").

182. *See, e.g.*, Minda Zetlin, *The 9 Weirdest and Most Hilarious Questions Congress Asked Mark Zuckerberg*, INC. (Apr. 12, 2018), https://www.inc.com/minda-zetlin/mark-zuckerberg-congress-hearings-funny-stupid-questions.html (displaying a significant lack of technical literacy on the part of legislators).

183. Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, HARV. BUS. REV. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data.

184. *Cf. id.* (discussing possible solutions involving giving users control over their own data).

185. *Id.*

186. *Data Privacy Hearing*, *supra* note 22, at 3 (testimony of Maureen K. Ohlhausen).

the latter, what would the bounds of "privacy tourism" be? A federal law is the best route to take for this level of protection.

A federal privacy law that emphatically bans the sale of data to third parties would address the risks that consumers face currently. In the event of a data breach, consumers would be on notice that their data were at risk because they are sharing with first parties only.[187] The age of unsolicited advertisements, misinformation, and democracy-threatening ads might be mitigated because the consumer would have control over who accesses their data and to what purposes it is put.[188] This blanket, bright-line rule is the best way to go forward to protect consumers with a legislative solution to the problem of data privacy in the online space in the United States.

B. The Best Way Forward for Companies

Another compelling reason to legislate a total ban on data sharing in the interest of private entities is the illusion of the stability of the online advertising industry. Data sharing is often cited as an essential part of offering online advertising.[189] However, value of online advertising is overblown by its proponents. For example, the Wall Street Journal discovered that Facebook inflated video ad watch time by 60–80% to ad purchasers for over two years.[190] Another study found that ad tech "middlemen" took as much as a 50% cut of ad spending.[191] Yet another study found that microtargeting, highly touted for accuracy, performed slightly worse than random guessing.[192] Because of the opacity of the online advertising industry, it is difficult to surmise its sustainability.

Tim Hwang argues that online advertising is a "bubble" that is bound to pop once the lack of value of online advertising is fully exposed.[193] Popping this bubble with legislation is much preferable to waiting until the market responds. First, private entities will have time to pivot.[194] Legislation would give at least a year, if not more, for companies to adjust their business models in response.[195] The alternative is to wait for the bubble to pop and let the online advertising market simply crash. Additionally, the market solutions that arise as a response

187. *Cf.* Nicolás Rivero, *The Digital Ad Industry Is Rewriting the Bargain at the Center of the Internet*, QUARTZ (Apr. 25, 2021), https://qz.com/2000490/the-death-of-third-party-cookies-will-reshape-digital-advertising (reviewing the basics of first-party data tracking and how it improves consumer privacy).

188. *Id.*

189. *See, e.g.*, *WhatsApp Privacy Policy*, WHATSAPP (Jan. 4, 2021), https://www.whatsapp.com/legal/updates/privacy-policy ("You share your information as you use and communicate through our Services, and we share your information to . . . market our Services.").

190. Suzanne Vranica & Jack Marshall, *Facebook Overestimated Key Video Metric for Two Years*, WALL ST. J. (Sept. 22, 2016, 7:29 PM), https://www.wsj.com/articles/facebook-overestimated-key-video-metric-for-two-years-1474586951.

191. Gilad Edelman, *Ad Tech Could Be the Next Internet Bubble*, WIRED (Oct. 5, 2020, 8:00 AM), https://www.wired.com/story/ad-tech-could-be-the-next-internet-bubble.

192. *Id.*

193. Subprime Attention Crisis, *supra* note 89.

194. *See California Consumer Privacy Act of 2018*, IAPP (Feb. 2021), https://iapp.org/resources/article/california-consumer-privacy-act-of-2018 (stating the Act was passed in 2018, but won't go into effect until 2020).

195. *Id.*

to drastic legislation will have time and space to be explored. Whether it is a pay-for-privacy model, a non-profit model such as Wikipedia, or something yet unexplored, there is potential for innovation in this space.

Even if the online advertising bubble does not pop soon, it would not be so difficult to pivot under this proposed law. A ban on sharing between private entities would not bar consumers from sharing their data multiple times with multiple entities, which they may be likely to do. Consumers seem to be more confident in sharing their data for some clear purposes, and not others. For example, 49% of consumers believe sharing student data with a nonprofit to improve educational outcomes is acceptable, while only 27% would consent to social media sites monitoring posts for signs of depression.[196] Similarly, in the EU, willingness to share information depends on the type of data: users are more willing to share information on consumption habits than health or wealth information.[197] We know that there are uses of big data in AI that have made significant contributions to society in areas like healthcare and scientific research.[198] Consumer attitudes in both the United States and the EU suggest that, in certain cases, users would be willing to share their data as long as it were used within the boundaries of clearly defined purpose limitations of the entity soliciting the data from users.

A practical reason to preempt state laws with a federal law is the cost of compliance. So far, the patchwork of state laws not only results in a lack of uniformity of data protections of U.S. citizens but also creates huge expenses for companies. As it stands, the cost of compliance with data protection regulations ranges from $7,000,000 to almost $40,000,000.[199] Even compliance does not ensure total protection from lawsuits, and so far, interpretations of the CCPA have made it difficult to predict exactly how to comply or what forms of data manipulation are allowed under the Act.[200] Additionally, this cost of compliance is often impossible for small businesses to meet, and many business owners oppose the law because of its complicated and unclear requirements.[201] Creating a federal law with a clear bright-line rule against sharing user data would reduce these astronomical costs.[202]

196. PEW, *supra* note 6.

197. Karampela et al., *supra* note 155, at 6509.

198. Lefkowitz, *supra* note 51.

199. GLOBALSCAPE, THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS 5 (2017), https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf.

200. Greg Bensinger, *So Far, Under California's New Privacy Law, Firms Are Disclosing Too Little Data—or Far Too Much*, WASH. POST (Jan. 21, 2020), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency.

201. Lawrence Chou, *New Privacy Rules, Lawsuit Abuse Crush California's Online Businesses*, TIMES SAN DIEGO (Jan. 14, 2021), https://timesofsandiego.com/opinion/2021/01/14/new-privacy-rules-lawsuit-abuse-crush-californias-online-businesses.

202. State privacy laws are also probably subject to the dormant commerce clause and, though unlikely, could be struck down as unconstitutional. In that event, consumers would be left unprotected, and companies would have essentially wasted their entire compliance investments. *See* Kiran Jevanjee, *Nice Thought, Poor Execution: Why the Dormant Commerce Clause Precludes California's CCPA from Setting National Privacy Law*, 70 AM. U.L. REV. F. 75, 132–33 (2020) (claiming that the CCPA could be struck down as unconstitutional).

Tech companies are not uniformly opposed to strict data protections for consumers.[203] Tim Cook, CEO of Apple, recognizes that consumers have a right to see where their information is being sold and to delete it if they so wish.[204] Though Cook seems to be in the minority of CEOs of tech companies,[205] it is important to note and question the support of federal privacy law from the perspective of tech companies. Tech companies have many more resources than individuals or public interest groups, and their lobbying potential is not to be underestimated.[206] If the microphone is solely in the hands of CEOs, it is unlikely that a data protection law will truly protect the interest of consumers. But it is important that a federal data privacy law treats all entities equally—consumers desire protection of their data from their local pet store as well as the social media giants. For this reason, a simple solution of no data sales creates a simplicity of compliance from entities small and large that no other solution has yet achieved.

A uniform data protection law that bans the sharing of data to third parties would offer a sustainable avenue for consumer protection as well as companies. This law would create time to address economic weaknesses and ultimately save costs in compliance. Using this categorical ban as a baseline for federal privacy legislation is the best and simplest solution for protecting consumer data privacy as it currently stands.

V. CONCLUSION

In the current state of privacy law, most Americans have almost no control over the uses and dissemination of their personal data. This lack of control is a violation of individual privacy rights, civil rights, and human rights.[207] Alternative technical solutions, such as opt-in requirements and differential privacy, will only further complicate the matter and will continue to muddy the waters of privacy law interpretation. State legislation, especially legislation that puts the onus on the consumer to protect data, will not adequately protect consumers and will create huge compliance costs for companies. The status quo of self-regulation by private entities cannot continue indefinitely without federal intervention. Moving forward, further research must be done on how to adequately advise private entities on pivoting away from online advertising. The deeply entrenched belief in the online advertising system will likely take significant effort to overcome.

A bright-line rule against sharing data, though drastic, is the only way to meet the desires of consumers and overcome the hurdles of compliance. The law certainly must have multiple provisions that repair previous harm done by a lack

203. Lapowsky, *supra* note 65.

204. *Id.*

205. Sara Salinas & Sam Meredith, *Tim Cook: Personal Data Collection Is Being 'Weaponized Against Us with Military Efficiency,'* CNBC (Oct. 25, 2018), https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html.

206. Jane Chung, *Big Tech, Big Cash: Washington's New Power Players*, PUB. CITIZEN (Mar. 24, 2021), https://www.citizen.org/article/big-tech-lobbying-update.

207. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

of data privacy, such as the right to be forgotten and transparent purpose limitations for uses of data. But a law that truly protects consumers' voices, demanding control over data, uses a total prevention of data sharing as a cornerstone for building sustainable data privacy protections. This bright-line rule would offer consumers the clarity they desire with regards to uses of data, and would allow companies to pivot away from online advertising sustainably and save substantial costs of compliance.