NOTES

THE OPTIMAL OPT-IN OPTION: PROTECTING VULNERABLE CONSUMERS IN THE EXPANDING PRIVACY LANDSCAPE

*Morgan Carter**

This Note addresses the ever-growing series of privacy laws being enacted throughout the United States and the danger that the "opt-out" data collection system poses to many populations. There is a disparity in the level of "digital literacy" throughout the United States, and as more consumer data privacy laws emerge and continue to replicate the existing legislation, that disparity deepens.

Patterns among who does and who does not opt out of data collection contribute to algorithmic bias. Access to consumer data can create discriminatory and unequal treatment, which may be exacerbated by disparities in participation in opt-out provisions, increasing the vulnerability of populations less aware of or educated about the potential dangers of data collection. It is crucial that the United States implement a more robust regulatory system regarding its opt-out provisions to protect those who are most vulnerable in the digital world.

* J.D. Candidate 2024, Columbia Law School. Endless thanks to Professor David Pozen for his guidance and encouragement, the *Columbia Law Review* staff for their editorial work, and my family for being my biggest supporters and my loudest cheerleaders.

INTRODUCTION

In May 2016, ProPublica found that risk scores used nationwide to predict whether a defendant will commit a crime in the future are biased against Black people.[1] In a study of 7,000 defendants, their risk scores, and their actual recidivism rates, "[w]hite defendants were mislabeled as low risk more often than [B]lack defendants."[2] For-profit companies like Equivant survey and collect data on defendants and then generate these biased risk scores.[3] Like most developers, their goal is to create a more efficient, productive system that prevents the introduction of human errors. "The trick, of course, is to make sure the computer gets it right."[4]

In 2019, Ziad Obermeyer—a professor at the University of California, Berkeley's School of Public Health—and his team were looking into how algorithms inform healthcare management in large hospitals.[5] Their research revealed not only a problem in the healthcare industry but the tip of a systemically racist iceberg. An algorithm that was widely used by hospitals in the United States to help allocate healthcare to the patients visiting the hospital was guilty of "systematically discriminating against [B]lack people."[6] The data from the hospital Obermeyer and his team studied showed that the people who self-identified as Black "were generally assigned lower risk scores than equally sick white people."[7] Black

1. Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, Machine Bias, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/7QDL-SGA4].

2. Id.

3. Id. Equivant previously conducted business under the name "Northpointe" after a 2017 rebrand. Press Release, Equivant, CourtView Justice Solutions Inc., Constellation Justice Systems Inc., and Northpointe, Inc. Announce Company Rebrand to Equivant (Jan. 10, 2017), https://www.einnews.com/pr_news/361378637/courtview-justice-solutions-inc-constellation-justice-systems-inc-and-northpointe-inc-announce-company-rebrand-to-equivant [https://perma.cc/6TD4-QKXT].

4. Angwin et al., supra note 1.

5. Heidi Ledford, Millions Affected by Racial Bias in Health-Care Algorithm, 574 Nature 608, 608 (2019).

6. Id.

7. Id.

patients, though equally sick, were wrongly considered to be in less urgent or immediate need of care than white patients.[8]

The information and data that are collected on people can be twisted and used in discriminatory ways. Now more than ever, "the amount and variety of data that is collected from individuals has increased exponentially, ranging from structured numeric data to unstructured text documents such as email, video, audio and financial transactions."[9] Companies use, sell, and share this information.[10] Further, law enforcement buys these data to build massive and discriminatory police surveillance networks.[11] All these personal datasets are summarized using a collection of methods identified by scholars as "Big Data analytics,"[12] and they can be used to inform companies and institutions on whether to approve a loan, grant parole, or deny a job application, among other things.[13] With access to Big Data, machine learning comes in to help uncover consumer trends and patterns with the help of decisionmaking algorithms.[14] Businesses find it helpful when these algorithms categorize and recognize patterns in the data that they can use.[15] Although the concepts of information and patterns on their own give the impression of impartiality, bias and racism thrive off Big Data analysts sharing and selling data.[16]

What, then, is being done about this? Only recently has the United States embarked on the journey of building privacy regulations and data-protection laws to protect the people who use varied technologies, social

---

8. See id. ("As a result [of discriminatorily assigned lower risk scores] . . . [B]lack people were less likely to be referred to the programmes that provide more-personalized care.").

9. Maddalena Favaretto, Eva De Clercq & Bernice Simone Elger, Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review, J. Big Data, Dec. 5, 2019, at 1, 2.

10. See Sarah Lamdan, Defund the Police, and Defund Big Data Policing, Too, Jurist: Acad. Comment. (June 23, 2020), https://www.jurist.org/commentary/2020/06/sarah-lamdan-data-policing [https://perma.cc/8EV2-JCMG] (identifying Thomson Reuters and RELX as massive data analytics corporations engaging in the surveillance and sale of personal data).

11. Id. ("[T]oday's policing infrastructure . . . spends millions of dollars on an invisible, sprawling data surveillance industry[,] . . . form[ing] oppressive systems that discriminate against communities of color, refugees, and migrants.").

12. Favaretto et al., supra note 9, at 2 (defining "Big Data analytics" as "the plethora of advanced digital techniques (e.g.[,] data mining, neural networks, deep learning, profiling, automatic decisionmaking and scoring systems) designed to analyze large datasets with the aim of revealing patterns, trends and associations, related to human behavior").

13. Id.

14. Chithrai Mani, How Is Big Data Analytics Using Machine Learning?, Forbes (Oct. 20, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/10/20/how-is-big-data-analytics-using-machine-learning [https://perma.cc/9NFV-RXHQ].

15. Id.

16. See infra section I.A.

media, and websites.[17] The United States has seen enormous transformation in terms of privacy regulation and steps taken to combat the potential dangers inherent in a society that is interwoven with the online world.[18] States have been stitching together the first wave of defenses against privacy infringements on a state-by-state basis.[19]

Five states have taken necessary steps to strengthen their data privacy laws. These states have created seemingly more robust and comprehensive legislation that establishes a standard for consumer privacy. This legislation is already being enforced in these five states: California, Colorado, Connecticut, Utah, and Virginia.[20] California led the way on these data privacy and consumer laws with the California Consumer Privacy Act (CCPA), and the other four followed suit, even using much of the same verbiage as the CCPA.[21] Much of this language addresses companies that collect data, mandating full disclosure of what data is being taken and whether it is being sold.[22] Additionally, these laws mandate opt-out provisions in an effort to allow people to take further individual control over whether their data can be sold or accessed.[23] Data and consumer privacy concerns are rapidly growing: At least thirty-five states and the District of Columbia introduced or considered almost two hundred consumer privacy bills in 2022.[24]

As these data privacy concerns and protections morph and transform so rapidly, companies and organizations are keeping a close eye on quickly evolving state regulations to stay on top of how they would need to respond

---

17. See infra sections I.B–.C.

18. See infra section I.D.

19. See id.

20. Andrew Folks, US State Privacy Legislation Tracker, Int'l Ass'n of Priv. Pros., https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/G7WL-8ADZ] (last updated Feb. 23, 2024) (presenting images and descriptions of state privacy legislation as it exists today, as well as when enacted laws will become effective and actually enforced).

21. California Consumer Privacy Laws, Bloomberg L., https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/ [https://perma.cc/XEK8-86FH] (last visited Jan. 12, 2023) (stating that the CCPA is the "first comprehensive consumer privacy legislation in the U.S." and may serve as a model for other states).

22. Thorin Klosowski, The State of Consumer Data Privacy Laws in the US (and Why It Matters), N.Y. Times: Wirecutter (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us (on file with the *Columbia Law Review*) (explaining that "a company operating under these regulations must tell you if it's selling your data").

23. Id. (describing the "global opt out" requirement).

24. Pam Greenberg, 2022 Consumer Privacy Legislation, Nat'l Conf. of State Legislatures, https://www.ncsl.org/research/telecommunications-and-information-technology/2022-consumer-privacy-legislation.aspx [https://perma.cc/4W9J-3CTY] (last updated June 10, 2022).

to such shifts. Law enforcement has already begun using data-driven predictive models to zero in on areas and communities likely to be involved in criminal activities.[25] Many of these data, which reflect preexisting biased arrest patterns, perpetuate the problem. Some policing in departments such as the Los Angeles Police Department (LAPD) has moved to "Big Data Policing," also called "data-informed community-focused policing" (DICFP).[26] Under this policy, law enforcement even coordinates directly with tech firms to surveil a person's presence online (social media postings), to investigate crimes, and to monitor what it would deem potential threats.[27] Before many of the consumer privacy regulations, tech companies were under little to no obligation to inform their users about how they were sharing their users' data or the ways their users' actions were being monitored.[28]

The emergence of the opt-out provision, specifically, returned some degree of agency to consumers over their privacy permissions and whether they allow a company to share or sell their data. In 2012, a story emerged detailing how Target was able to predict people's pregnancies before they had so much as told their families.[29] These predictions were possible thanks to a statistician, "predictive analytics," and unfettered access to consumer data.[30] Consumer data privacy and the right to opt out emerged after such events, and those who seek it out may exercise some agency to

---

25. See Johana Bhuiyan, LAPD Ended Predictive Policing Programs Amid Public Outcry. A New Effort Shares Many of Their Flaws, The Guardian (Nov. 8, 2021), https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform [https://perma.cc/H8A4-6N3R] (discussing how new Los Angeles Police Department predictive policing programs "bear[] a striking resemblance" to past data-driven programs that came under immense scrutiny for disproportionately leading to overpolicing in Black and brown communities).

26. Id.; see also Sarah Brayne, Dye in the Cracks: The Limits of Legal Frameworks Governing Police Use of Big Data, 65 St. Louis U. L.J. 823, 826–28 (2021) (describing how the LAPD uses big data to surveil both the general population and suspects).

27. Sam Levin, Revealed: LAPD Officers Told to Collect Social Media Data on Every Civilian They Stop, Guardian (Sept. 8, 2021), https://www.theguardian.com/us-news/2021/sep/08/revealed-los-angeles-police-officers-gathering-social-media [https://perma.cc/4M5B-NL5D] (explaining how LAPD officers were told it was critical to collect civilian social media data for use in "investigations, arrests, and prosecutions") (quoting Memorandum from Michel R. Moore, Chief of Police, L.A. Police Dep't, to All Department Personnel, L.A. Police Dep't 1 (July 22, 2020), https://www.brennancenter.org/sites/default/files/2021-09/I.%20Beck%20FI%20Memo.pdf [https://perma.cc/LWZ9-PSW2])).

28. See Alison Divis, How the CCPA Benefits Consumers and Business Owners, Pac. Data Integrators, https://www.pacificdataintegrators.com/insights/ccpa-benefits [https://perma.cc/MYF3-WA7Q] (last visited Jan. 15, 2023) (explaining how the CCPA was set to change the privacy landscape).

29. Charles Duhigg, How Companies Learn Your Secrets, N.Y. Times (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (on file with the *Columbia Law Review*).

30. See id. (identifying these three factors as central reasons for Target's successful predictions).

avoid similar situations. At least, that is the perception. Virtually all the enhanced-privacy and consumer protection regulations relevant here were passed within the previous three years, and countless more are inevitably on the horizon.[31] In the flurry of new laws both passed and upcoming, no one has thoroughly evaluated how effective these regulations are at avoiding these potential avenues of racism and bias. The opt-out provisions found within each of the new regulations contain "antidiscrimination" sections, but the language therein is thin and leaves many questions unanswered.[32] Is allowing for opt-out provisions and providing antidiscrimination language really benefitting diverse and marginalized communities? Or is it merely cementing the position of surveillance and tracking in our society while just making it transparently known that this is the status quo?

These new privacy laws' variety and novelty raise questions about their effectiveness and the impact that they actually have. Since machine learning of people's behaviors and preferences leads to wide-scale algorithmic bias, certain consumers opting out has also impacted the machine learning's algorithmic process. That is to say, there is algorithmic bias based on who *does* opt out versus who *does not*. Access to consumer data can create discriminatory and unequal treatment, which may be exacerbated by disparities in participation in opt-out provisions, increasing the vulnerability of populations less aware of or less educated about the potential dangers. It is crucial that the United States implement a more robust regulatory system regarding its opt-out provisions to protect those who are most vulnerable in the digital world.

This Note starts in Part I with a discussion of the history of discrimination enabled by a lack of data privacy. Part I then turns to state-specific privacy regulations, providing a general overview of the key rights found in these regulations and discussing the regulations' strengths. Part II looks at the laws as they are applied and breaks down the ways that the regulations may generate discrimination based on who decides to opt out. Part III addresses potential remedies in the form of a national privacy framework; mandated opt-in provisions in place of opt-out provisions; and altered presentation of the existing opt-out website pop-ups to make them both easy to understand and unavoidable by consumers.

I. CONSUMER PRIVACY AND DISCRIMINATORY ALGORITHMS

A. *Racial Discrimination in Consumer Data Collection and Sharing Practices*

People of color have to fight against bias and systemic racism that have most recently manifested themselves in the form of algorithms and the use of

---

31. See Greenberg, supra note 24 (providing an overview of the progression of consumer privacy legislation).

32. See infra section I.D.3.

consumer data.[33] There is a distinct trend of Black and brown people being "stripped of equitable opportunities in housing, schools, loans, and employment because of biased data."[34]

Public policy executive and social scientist Dominique Harrison enumerates the ways that Black and brown people have seen the direct and negative impacts of the problematic use of consumer information, including its use in voter suppression and racial targeting. In the 2016 elections, for instance, "[t]he Russian Internet Research Agency (IRA) used voter suppression tactics on online platforms, such as Twitter, Facebook, Instagram, and YouTube[,] to influence African Americans" and spread misinformation to those targeted communities.[35] The bias in corporate algorithms has also been the cause of targeted and racist marketing policies and practices used by tech companies.[36]

In 2019, HUD sued Facebook for permitting advertisers to market to groups characterized by race, gender, and religion with the use of ad-targeting tools and algorithms.[37] As a result of the biased algorithm, "[a]ds about homes for sale were . . . shown to more white users, while ads for rentals were shown to more minorities."[38] Consumer data includes information such as one's age, gender, race, recent purchases, social media engagement, website visits, most viewed pages, and more.[39] The bias comes in during the collection and resulting utilization of this data, and some believe that these algorithms and Big Data are likely "making the world worse by accelerating the problems in the world that make things unjust."[40]

Many perceived the emergence of consumer privacy regulations to be an optimistic opportunity to hold companies accountable for sharing, selling, and using consumer data.[41]

---

33. See Dominique Harrison, Civil Rights Violations in the Face of Technological Change, Aspen Inst. (Nov. 2019), https://www.aspeninstitute.org/blog-posts/civil-rights-violations-in-the-face-of-technological-change [https://perma.cc/5ZH8-KMTH] (last updated Oct. 22, 2020) (providing examples and an analysis of the ways that discrimination from technology algorithms impacts communities of color).

34. Id.

35. Id.

36. Id.

37. Karen Hao, Facebook's Ad-Serving Algorithm Discriminates by Gender and Race, MIT Tech. Rev. (Apr. 5, 2019), https://www.technologyreview.com/2019/04/05/1175/facebook-algorithm-discriminates-ai-bias [https://perma.cc/U6SL-977N].

38. Id.

39. Indrajeet Deshpande, What Is Customer Data? Definition, Types, Collection, Validation and Analysis, Spiceworks, https://www.spiceworks.com/marketing/customer-data/articles/what-is-customer-data [https://perma.cc/5KB7-SXTN] (last updated Mar. 16, 2021).

40. Hao, supra note 37 (internal quotation marks omitted) (quoting Christian Sandvig, Director of the Center for Ethics, Society, and Computing at the University of Michigan).

41. See, e.g., Cyrus Farivar & David Ingram, California's New Data Privacy Law Could Change the Internet in the US, CNBC (May 14, 2019), https://www.cnbc.com/2019/05/14/

In the consumer rights provisions provided within regulations such as the Biometric Information Privacy Act (BIPA), the CCPA, the California Privacy Rights Act (CPRA), and the Colorado Privacy Act (CPA), there was hope of resolution and additional protections to guard against such injustices as these for marginalized communities. On the other hand, there was also awareness that businesses may instead "find ways around the requirements."[42]

B. *The Evolution of Privacy Regulation in the United States*

The present wave of privacy regulation comes as today's world finds itself increasingly online, be it with social media, shopping, or even banking. The United States lacks one singular, comprehensive data privacy law or framework, like the European Union's General Data Protection Regulation (GDPR). Rather, the United States has regulated data privacy on a state-by-state basis, starting with the CCPA. The sheer number of varying data privacy laws being enacted during such a short period of time might come across as confusing. That being said, it also sends the message to businesses that protecting consumer data is a priority, even if it has to be done in a piecemeal way. Amie Stepanovich of the Silicon Flatirons Center described this process as "raising the water level" and added that "companies often choose 'to apply the stronger, more protective standard across the board for everyone' when legal standards go up."[43] While these legal standards improve, the objective must be to create and also preserve a system that does not create wide inequities and perpetuate discrimination at the same time.

The right to opt out of data sharing and selling is one of the many provisions of the evolving statewide privacy protection framework that has persisted in many states' data privacy regulations following the CCPA.[44] When consumers know about and consequently opt out of the sharing, selling, or use of their personal data, agency is returned to the consumer and a leash is put on corporations that have been known to abuse this access in the past.

---

california-consumer-privacy-act-could-change-the-internet-in-the-us.html [https://perma.cc/K9D5-LNAW] ("Consumer advocates say the [California Consumer Privacy Act] could meaningfully improve online privacy without losing what people like best about the internet.").

42. Id.

43. Klosowski, supra note 22.

44. See Robb Hiscock, The Ultimate Guide to US Privacy, OneTrust (Dec. 9, 2022), https://www.onetrust.com/blog/the-ultimate-guide-to-us-privacy [https://perma.cc/XMK4-DEKN] (outlining the opt-out provisions common across six new state privacy laws following the passage of the CCPA).

C. *The General Consumer Data Privacy Landscape Before More Comprehensive Privacy Regulations*

As the CCPA was being analyzed during its enactment in 2020, discussion arose as to how the new legislation was going to affect consumers' lives.[45] Other camps wondered whether it would even be effective in the fight to protect privacy.[46]

Before the enactment of the CCPA, the internet in the United States was its own version of a Wild West, void of comprehensive data privacy regulations allowing consumers agency in how and why their data were used.[47] In 2019, a research study showed that most Americans navigated their daily lives with the belief that their data were constantly being tracked but the feeling that they had very little or no control over that reality.[48] Additionally, most Americans felt they lacked understanding about what data collection does and how it affects them.[49] Many did not realize the gravity of data privacy protections until the Facebook Senate hearing with Mark Zuckerberg in 2017. The hearing revealed that Cambridge Analytica, along with many other firms working with Facebook, had been allowed to access data and information of up to eighty-seven million Facebook users worldwide without their consent.[50]

In the midst of consumers' confusion and misunderstanding, discriminatory practices such as the denial of "credit cards to consumers based on

---

45. See Geoffrey A. Fowler, Don't Sell My Data! We Finally Have a Law for That, Wash. Post (Feb. 19, 2020), https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq (on file with the *Columbia Law Review*) (discussing the CCPA's impact on consumers and common questions about the law); Rachel Lerman, California Begins Enforcing Digital Privacy Law, Despite Calls for Delay, Wash. Post (July 1, 2020), https://www.washingtonpost.com/technology/2020/07/01/ccpa-enforcement-california (on file with the *Columbia Law Review*) ("It gives consumers in the state . . . broad ability to be able to request that companies tell them what personal data they hold on each person and to ask companies to stop selling their personal data to third-party advertisers or others.").

46. See Fowler, supra note 45 (discussing the way in which "[p]rivacy advocates have mixed feelings about the CCPA").

47. See id. (arguing that the CCPA is "America's first broad data privacy law" and gives people the power to control more of how corporations gather and sell consumer data than did previous regimes).

48. See Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [https://perma.cc/SNG5-LLAY] (polling Americans and finding that a majority feel that most of their online activity is being tracked but they have little-to-no control over their data).

49. Id.

50. Paolo Zialcita, Facebook Pays $643,000 Fine for Role in Cambridge Analytica Scandal, NPR (Oct. 30, 2019), https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal [https://perma.cc/Y84T-F5VQ].

language proficiency and ethnicity" were carried out through "discriminatorily constructed algorithms."[51] Furthermore, marginalized communities felt several other types of harm, "such as abusive lending practices and housing discrimination that has stopped people of color from building wealth through homeownership."[52]

D. *The Emergence of the CCPA, the CPRA, the CPA, and the BIPA*

1. *Origin and Purpose of the Privacy Acts.* — The CCPA was a ballot initiative in 2018 and was continually amended over the course of the next year.[53] Some of the initial amendments included the changing of the definition of "personal information" and exemptions of certain parties from some of the personal information and opt-out obligations of the CCPA.[54] The law went into effect on January 1, 2020, and was enforceable as of July 1, 2020.[55] The CCPA is extensive and far-reaching, with comprehensive definitions of "personal information," "data sharing," and "data selling" and also finds an expansive area of generality in terms of the businesses that it affects. The CPRA builds on the CCPA, closing some of the gaps left by the CCPA while leaving some entities untouched by either law. The legislation went into effect on January 1, 2023, and is enforced by the first, though presumably not last, data privacy protection agency in the country: the California Privacy Protection Agency (CPPA).[56] The primary function of the CPPA is that it "mandates all businesses to audit their data collection, storage, processing and sharing mechanisms."[57] In Colorado, the CPA was signed on July 7, 2021, and took effect on July 1, 2023.[58] The CPA

---

51. Valencia Richardson, Note, Data-Driven Discrimination: A Case for Equal Protection in the Racially Disparate Impact of Big Data, 12 Geo. J.L. & Mod. Critical Race Persps. 209, 210 (2020).

52. Abi Velasco & Remington A. Gregg, Pub. Citizen, Racial Equity & Consumer Protection 4 (2022), https://www.citizen.org/wp-content/uploads/Racial-Equity-Consumer-Protection-Issue-Brief_final_1-19-22-page-numbers.pdf [https://perma.cc/9LSW-LJMS].

53. See California Consumer Privacy Act, PrivacyRights.org (Jan. 6, 2020), https://privacyrights.org/resources/california-consumer-privacy-act [https://perma.cc/6KEQ-4C5E] (providing a history of the CCPA from ballot initiative to passage to subsequent amendment).

54. See id. (observing that the definition of "personal information" was amended to "specifically exclude de-identified and aggregate information" and other exemptions from the law included data indicating illegal activities, employment data, and data protected under other statutory schemes, such as medical information).

55. Id.

56. Anas Baig, California Privacy Rights Act (CPRA), Securiti (Mar. 1, 2022), https://securiti.ai/what-is-california-privacy-rights-act-cpra [https://perma.cc/6KVB-76GP] (last updated Dec. 13, 2023).

57. Id.

58. 2021 Colo. Sess. Laws 3445; Colorado Privacy Act (CPA), Phil Weiser: Colo. Att'y Gen., https://coag.gov/resources/colorado-privacy-act [https://perma.cc/252S-E3TX] (last visited Jan. 19, 2024).

is said to be "a bit stricter than the [Virginia Consumer Data Privacy Act] and a bit more lenient than the CCPA."[59] In many ways, the CPA borrows pieces from the CCPA, while in others it is a complete departure. For instance, one area of similarity is found in the Act's definition of "sale," wherein a sale occurs when the personal information is exchanged for "monetary or other valuable consideration."[60] "In this sense, the CPA is more similar to the CCPA because controllers will be left to ponder what is 'other valuable consideration.'"[61] Even before these more recent pushes for privacy, the BIPA was enacted in Illinois in 2008.[62] The first enactment of its kind in the nation, the BIPA covers "entities that use and store biometric identifiers" and forces them to "comply with certain requirements" in their process of doing so while also providing a private right of action if the entities do not comply.[63] States like Washington and Texas also have biometric information protection laws, but they lack the private right of action component and are less expansive.[64] These four privacy regulations represent the variety of privacy and consumer data regulations being enacted across the country. In many ways, they overlap and even contain the same language. In many other ways, however, they depart from one another, charting their own paths in the privacy space and leaving future states to pick and choose the regulatory language they adopt. Two crucial provisions found in these regulations are the opt-out provision and the right to nondiscrimination.

2. *The Right to Opt Out.* — The opt-out right was at the heart of California's recent settlement with makeup brand Sephora after the state said the company "failed to follow opt-out requests that its customers made via browser privacy controls."[65] The case came as a shock to many, exhibiting the financial repercussions that companies could risk by violating privacy regulations.

---

59. Sarah Rippy, Colorado Privacy Act Becomes Law, Int'l Ass'n of Priv. Pros. (July 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law [https://perma.cc/GJM7-24NZ].

60. Colo. Rev. Stat. § 6-1-1303(23)(a)–(b) (2023). "De-identified data" are also defined as data that cannot be reasonably used to draw conclusions about or to link to an identified or identifiable individual. See id. § 6-1-1303(11).

61. Rippy, supra note 59.

62. Is Biometric Information Protected by Privacy Laws?, Bloomberg L. (May 3, 2021), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits [https://perma.cc/WDB4-29VY].

63. Id.

64. See id. (expanding upon the ways in which Illinois, Texas, and Washington biometric privacy statutes differ from one another).

65. Tom Chavez, Sephora's $1.2 Million Fine Proves Customer Privacy Is an Innovation Imperative, Forbes (Oct. 27, 2022), https://www.forbes.com/sites/tomchavez/2022/10/27/on-privacy-regulators-are-awakening-the-consumerand-its-an-innovation-imperative (on file with the *Columbia Law Review*).

The CCPA includes "opt-out" provisions that permit a consumer to "direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information."[66] Additionally, when businesses sell consumers' personal information to a third party, they are obligated to provide consumers with explicit notice that the information is being sold, along with the option to opt out of sale.[67] A degree of agency is given back to consumers here, allowing them to revoke businesses' ability to sell their information to a third party. The CCPA's data sharing and selling provisions require that businesses provide "a clear and conspicuous link on the business's internet homepages, titled 'Do Not Sell or Share My Personal Information,' to an internet web page that enables a consumer . . . to opt-out of the sale or sharing of the consumer's personal information."[68] It must be clear and accessible for consumers to find and use said link in order to opt out of the sale of their personal information. The CPRA uses this language while also adding the right to limit a business's use of Sensitive Personal Information (SPI), which "can compel corporations to limit the use of special categories of personal data," and an enhanced right to opt out, wherein the option to opt out of having personal information sold or shared is extended to cross-context behavioral advertising.[69] Furthermore, businesses need to update their privacy policies to let users know "if they plan to 'share' their data in addition to 'selling' their data. Under the CCPA, companies only needed to let users know if they planned on selling their data."[70]

The CPA's opt-out language mirrors that of the CCPA and the CPRA, ensuring that a consumer has the right to opt out of the processing of their personal data for uses outlined within the provision.[71] But the CPA opt-out right contains a provision not found in the CCPA. Consumers have the right to opt out of the processing of personal data for the purposes of targeted advertising, sale of personal data, or "profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."[72] As will be discussed in Part III, the scope and impact of this "profiling" language is largely unclear.[73]

---

66. Cal. Civ. Code § 1798.120 (2023).

67. Id. § 1798.115.

68. Id. § 1798.135.

69. Baig, supra note 56.

70. Id.

71. See Colo. Rev. Stat. § 6-1-1306(1)(a)(I) (2023) (granting the consumer the right to "opt out of the processing of personal data" related to "[t]argeted advertising," "sale of personal data," or "[p]rofiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer").

72. Id.

73. See infra Part III.

Importantly, the BIPA also prevents the disclosure or dissemination of a person's biometric information to another entity unless: the subject or their legal representative consents to the disclosure; the "disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information"; the disclosure is required by State or federal law; or the disclosure is required pursuant to a valid warrant or subpoena.[74] The BIPA does not have explicit opt-out language, though this is likely because it functions more like an "opt-in" system in which the consumer must explicitly consent for the information to be shared.[75]

3. *The Right to Nondiscrimination.* — With respect to the right to nondiscrimination, the CCPA states:

> (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:
>
> (A) Denying goods or services to the consumer.
>
> (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
>
> (C) Providing a different level or quality of goods or services to the consumer.
>
> (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
>
> . . . .
>
> (2) Nothing in this subdivision prohibits a business . . . from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.[76]

In addition to the above provisions, a business is allowed to offer consumers a financial incentive for the sale, sharing, or retention of their data, so long as doing so is not unfair, unjust, or coercive.[77] The purpose of the nondiscrimination language found here is to prevent repercussions against consumers who decide to exercise the rights they are allowed within these statutes. The CPRA, too, contains this language and sets out to protect these same consumer rights. It also adds that it is permissible for a business to offer loyalty or rewards programs for those who do choose

74. National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. § 3(d) (2020).

75. Id.

76. Cal. Civ. Code § 1798.125 (2023).

77. Id. § 1798.125(b).

to opt in, so long as the program remains consistent with the rest of the section.[78]

The CPA also includes a duty to avoid unlawful discrimination, but it additionally states that a business may not be prohibited from "offering a different price, rate, level, quality, or selection of goods or services to a consumer . . . if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount, or club card program."[79] So long as the price staggering or quality of service offered is related to the program offered, the separation of services there is lawful.[80] As stated in the CCPA and the CPRA, however, offering these staggered services based on whether a consumer permits the sharing, selling, or collection of their data without having a reasonably related reason for doing so would be unlawful.[81]

Contrary to the CCPA, the CPRA, and the CPA, the BIPA does not contain language around nondiscrimination surrounding the consent of personal biometric data and the exercise of one's rights related to this section. This is due to the nature of the BIPA, which is less about the consent surrounding the biometric data collection, and more about the processes required in obtaining and retaining it.[82]

E. *The Evolution of the Data Privacy Landscape After Additional Privacy Legislation*

In 2020, Facebook agreed to a $650 million settlement, one of the largest consumer data privacy settlements in U.S. history.[83] The claims alleged that Facebook had been subjecting users to facial recognition technology without user consent in violation of the BIPA.[84] The settlement served as a wake-up call that businesses must take privacy regulations seriously and update their processes to be in alignment with the regulations, or they could face monetary consequences. Similarly, the BIPA provision creating a private right of action has been affirmed as applying so that "[a]ny person aggrieved by a violation of th[e] Act shall have a right of

78. Id. § 1798.125(e).

79. Colo. Rev. Stat. § 6-1-1308(1)(d) (2023).

80. Id.

81. Cal. Civ. Code § 1798.120.

82. See Is Biometric Information Protected by Privacy Laws?, supra note 62 (outlining the functionality and purpose of the BIPA).

83. Id.

84. Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019) ("Plaintiffs' complaint alleges that Facebook subjected them to facial-recognition technology without complying with an Illinois statute intended to safeguard their privacy.").

action in a State circuit court."[85] By giving this power back to consumers, businesses are held accountable for the ways they collect, sell, and share data.

The CCPA's inclusion of the right to opt out of data sharing and its mandate that companies provide notice and information of how consumer data are sold and shared in turn allows consumers to make an informed choice to exclude themselves from the process of data collection and sharing. Advertising technology companies have had to comply with the new regulations, and the results of their compliance are apparent.

The Meta Platforms' quarterly report form explained that regulations like the CCPA have impacted the company's ability to generate targeted advertisement materials and revenue through their ads:

> [A]dvertising revenue has been, and we expect will continue to be, adversely affected by reduced marketer spending as a result of limitations on our ad targeting and measurement tools arising from changes to the regulatory environment and third-party mobile operating systems and browsers.
>
> In particular, legislative and regulatory developments such as the General Data Protection Regulation, ePrivacy Directive, and California Consumer Privacy Act have impacted our ability to use data signals in our ad products, and we expect these and other developments such as the Digital Markets Act will have further impact in the future. As a result, we have implemented, and we will continue to implement, changes to our products and user data practices, which reduce our ability to effectively target and measure ads.[86]

While not ideal for the company's bottom line, this response shows that companies like Meta are attempting to abide by the CCPA and other privacy regulations and feeling the heat from moving away from their previous data collecting, selling, and sharing techniques. The loss of profits in the existing privacy landscape could provide an incentive for additional creativity in both interpretation and application of the privacy regulations.[87]

Because the privacy environment will only continue to morph as additional regulations are passed and enforced nationwide, there is the possibility that online platforms and businesses that make use of

---

85. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1207 (Ill. 2019) (holding that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act").

86. Meta Platforms, Inc., Annual Report (Form 10-Q), at 33 (Oct. 26, 2022), https://www.sec.gov/Archives/edgar/data/1326801/000132680123000013/meta-20221231.htm [https://perma.cc/F93S-RSXJ].

87. See, e.g., Sara Quach, Park Thaichon, Kelly D. Martin, Scott Weaven & Robert W. Palmatier, Digital Technologies: Tensions in Privacy and Data, 50 J. Acad. Mktg. Sci. 1299, 1299–300 (2022) (acknowledging the financial burden that privacy regulations place on firms and proposing strategies that balance firm, consumer, and regulatory interests).

consumers' personal information will find and use loopholes. Businesses are increasingly likely to try to "find ways around the requirements."[88] Attempted avoidance is even more likely considering that the total absence of federal data privacy regulations means that businesses need to be "privy to the nuances" of each state's privacy regulations in a "rapidly changing ad tech industry."[89] Motivations like these, coupled with an ability to infer information about the parties who are less likely to opt out of data collection and sale, could create a fertile ground for inequality and exploitation of the data collected.

II. THE IMPACT OF THE RIGHT TO OPT OUT

A. *Who Is Left Behind in the Opt-Out System*

The topic of data privacy is relatively new; details and information about it are constantly updating and evolving. Comprehension of what personal data collection entails varies, and while it may be a cause of anxiety for some, others seem either apathetic or resigned about who has their data and where it goes.[90] Sixty-two percent of American adults believe that it is impossible to navigate daily life without companies collecting their data.[91] Even given this, nearly eighty percent are concerned about the way that companies use their data.[92] When surveyed about six different forms of personal information, only a very small percentage felt that they had a lot of control over who can access their personal information.[93]

Some of this disconnect could likely be attributed to a degree of digital literacy. Digital literacy is "the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills."[94] The term encapsulates the way that being able to find, create, and share digital

88. Farivar & Ingram, supra note 41.

89. Meaghan Donahue, What Do State Privacy Laws Mean for the Ad Tech Industry?, New Am. (Aug. 17, 2021), https://www.newamerica.org/oti/briefs/what-do-state-privacy-laws-mean-for-the-ad-tech-industry [https://perma.cc/PJS9-GGNZ].

90. See Auxier et al., supra note 48.

91. Id.

92. Id.

93. Id. The six different forms of personal information inquired about within the survey were: physical location; posts, activities, or social media; private conversations online and text messaging; purchases made online and in person; websites visited; and search terms used online. Id.

94. Liana Loewus, What Is Digital Literacy?, EducationWeek (Nov. 8, 2016), https://www.edweek.org/teaching-learning/what-is-digital-literacy/2016/11 [https://perma.cc/3FQY-ZWFR] (internal quotation marks omitted) (quoting the American Library Association's digital-literacy task force).

content online is a skill of increasing importance today.[95] Digital literacy can also help one to understand online safety, including what to share online and how that can affect one's privacy and reputation.[96]

Recognizing "dark patterns" is one example of digital literacy, and "individuals of high digital literacy are more likely to be able to identify and avoid falling trap to dark patterns."[97] On the other hand, "[s]tudies have shown that certain groups are more susceptible to dark patterns, such as communities of color, lower income individuals, children, older adults, and other historically disadvantaged groups."[98] In the workforce, digital gaps and lack of digital literacy disproportionately affect people of color "in large part due to structural factors that are the product of longstanding inequities in American society, such as income and wealth gaps and uneven access to high-quality K-12 education."[99] Seventeen percent of Black workers, thirty-two percent of Latino workers, and ten percent of Asian American and Pacific Islander workers have no digital skills at all.[100]

As a result of this significant split, there is valid concern that this digital literacy trend extends to other areas of digital privacy, such as taking action to opt out of the sharing, selling, or use of personal information. The Pew Research Center's survey states that only "50% of white Americans feel they have control over who can access information about their on- and offline purchases, compared with 69% of [B]lack adults and 66% of Hispanic adults."[101] Considering this difference in conjunction with the fact that so many people of color also struggle with digital literacy, an important question arises: Are people of color more confident over their online control because they are proactively taking charge in an area of concern; or has a lack of digital literacy has created a sense of false confidence because they do not know that digital privacy is an area where there should *be* concern?

The specific data on who opts out is inherently harder to locate since those who opt out remove their data and personal information from the flow of information. A study published in 2020, however, was able to find

---

95. See id. (examining the diverse ways in which digital literacy facilitates social engagement).

96. Id.

97. Catherine Zhu, Dark Patterns—A New Frontier in Privacy Regulation, Reuters (July 29, 2021), https://www.reuters.com/legal/legalindustry/dark-patterns-new-frontier-privacy-regulation-2021-07-29 [https://perma.cc/C2QF-Z4Y6]. "Dark patterns," or the purposeful action by a business of manipulating a consumer to obscure or impair their own autonomy, is one of the dangers that consumer privacy laws have sought to remedy. Id.

98. Id.

99. Nat'l Skills Coal., Applying a Racial Equity Lens to Digital Literacy 1 (2020), https://files.eric.ed.gov/fulltext/ED607424.pdf [https://perma.cc/DEW9-VTED].

100. Id. at 1–2.

101. See Auxier et al., supra note 48 (retaining the word "Hispanic" as used in the original source).

that while opt-out rates are generally very high for higher-income individuals, as well as older populations, the opt-out rate "falls with both the Asian- and African-American population shares."[102] Additionally, while there was a higher rate of ad blocker software use in the Asian American group (indicating an alternative form of privacy protection), the data show African Americans were less likely to use ad blocking.[103] African Americans may therefore disproportionately lack any substantive form of privacy protection while also being less likely to opt out of data sharing.

If people of color, and specifically Black people, are not opting out of data sharing, their data increase in importance to businesses profiting off the trade of consumer data. The overall increase in parties opting out means that the remaining consumers who have not opted out are increasingly valuable.[104]

B. *Exacerbating Factors*

As discussed below, businesses have an incentive to find ways to be creative around the opt-out provisions in privacy regulations.[105] In April 2021, Apple released iOS 14.5, which mandated users' permission to utilize certain tracking features as a result of the App Tracking Transparency policy.[106] Ninety-six percent of U.S. users decided to opt out.[107] Consumers who exercise their right to opt out generate fifty-two percent less revenue compared to consumers who do not.[108] The impact of privacy regulation on these companies' data-related profits is being recognized as tremendous.[109]

1. *Dark Patterns.* — Tactics such as dark patterns were previously a means by which businesses would both capture and retain consumer information.[110] Now, the CPRA dictates that an "'agreement obtained through

---

102. Garrett A. Johnson, Scott K. Shriver & Shaoyin Du, Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?, 39 Mktg. Sci. 33, 48 (2020).

103. Id.

104. See Guy Aridor, Yeon-Koo Che & Tobias Salz, The Effect of Privacy Regulation on the Data Industry: Empirical Evidence From GDPR 4 (Nat'l Bureau of Econ. Rsch., Working Paper No. 26900, 2022), http://www.nber.org/papers/w26900.pdf [https://perma.cc/QY83-M5S7].

105. See infra section II.B.3.

106. Samuel Axon, 96% of US Users Opt Out of App Tracking in iOS 14.5, Analytics Find, Ars Technica (May 7, 2021), https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find [https://perma.cc/8CDY-C344].

107. Id.

108. Johnson et al., supra note 102, at 34.

109. See Axon, supra note 106 ("It seems that in the United States, at least, app developers and advertisers who rely on targeted mobile advertising for revenue are seeing their worst fears realized . . . .").

110. See supra note 97 for a discussion of dark patterns and the dangers they pose to consumer privacy.

use of dark patterns does not constitute consent[]' and prohibits businesses from employing dark patterns to obtain a user's consent to resume data processing once a user chooses to opt-out."[111] This is the same case for the Colorado Privacy Act.[112] But the definition of "dark pattern" is still emerging, so space exists for businesses to push the boundaries—by making opt-in buttons more aesthetically appealing or obvious than opt-out buttons or otherwise finding means to try to retain more consumers, for example.[113]

As discussed in section II.A, people with higher digital literacy levels are better equipped to evade dark patterns. This would further perpetuate the problem in which those who remain opted in are disproportionately people of color, low-income, or of a marginalized community.[114]

2. *Ambiguous Language*. — A provision found in the CPRA prohibits discrimination between those who opt out and those who do not though a price or service difference can still be permissible "if that difference is reasonably related to the value provided to the business by consumer's data."[115] The determination of "how that value will be calculated is anyone's guess," however.[116]

One example of how this scenario comes into play is if a business were to offer both a free service and a premium, paid service. Antidiscrimination regulations would prohibit a business from permitting only the users who have the premium, paid service to exercise their privacy rights (for example, right to know, right to delete, right to correct).[117] If the business were to claim that the "premium payment is reasonably related to the value of the consumer's data to the business," however, then this would no longer be impermissible.[118] One such means of showing this

111. John J. Rolecki, Trends in Data Privacy Regulation: Dark Patterns, Nat'l L. Rev. (May 27, 2022), https://www.natlawreview.com/article/trends-data-privacy-regulation-dark-patterns [https://perma.cc/5CYY-2FNT] (quoting Cal. Civ. Code § 1798.140(h) (2023)).

112. Id.

113. David Stauss & Stacey Weber, How Do the CPRA, CPA, and VCDPA Treat Dark Patterns?, Husch Blackwell (Mar. 16, 2022), https://www.bytebacklaw.com/2022/03/how-do-the-cpra-cpa-and-vcdpa-treat-dark-patterns [https://perma.cc/9Q28-54QN] ("Precise definition and regulation of dark patterns is still emerging.").

114. See supra section II.A.

115. See Cal. Civ. Code § 1798.125.

116. CPRA and CCPA Compliance: What You Need to Know, Part & Sum, https://www.partandsum.com/blog/ccpa-compliance-what-you-need-to-know [https://perma.cc/XLY9-76DE] (last visited Dec. 28, 2022).

117. Alysa Z. Hutnik, Aaron J. Burstein & Alexander I. Schneider, The CCPA Non-Discrimination Right, Explained, Kelley Drye (Apr. 29, 2020), https://www.adlawaccess.com/2020/04/articles/the-ccpa-non-discrimination-right-explained [https://perma.cc/B2F6-VK4D]. The California Attorney General has also provided examples of how businesses may calculate the value of consumers' data in order to determine a reasonable price or service difference for users who do allow use of those data. Id.

118. Id.

value would be for a business to "determine that the payment for the premium version offsets the revenue provided by placing ads in the free version."[119] In such a case, the bar on discriminatory practices based on opt-out decisions seems fairly easy for a business to overcome, despite their prohibition.

An additional area of ambiguity rests within the understanding of "profiling" and the applications regarding automated decisionmaking. The CPRA, in amending the CCPA, addressed automated decisionmaking and "profiling consumers based on their 'performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.'"[120] Consumers can opt out or restrict the processing of their sensitive personal information for the purpose of profiling, but it's still unclear what implementation, or the result of requesting to opt out, would look like.[121] "It's questionable whether, for instance, the CPRA would disallow the infamous Target case," in which the company was able to determine and reveal to a teenager's family that she was pregnant.[122] Furthermore, there is varied understanding as to what would constitute "sensitive" personal information, especially in a world as rapidly evolving as our own.[123] Such confusion in distinguishing sensitive information from other categories of information can be seen in cases such as "emerging advancements in voice analysis that promise to discern an individual's COVID-19 status through the sound of their cough."[124] While the CPRA is designed to protect sensitive personal information, the specific details around what that entails and how far that protection extends are still being decided.

Ambiguities and potentially vague language, coupled with the newness of these regulations, mean that implementation and enforcement are still being configured, and businesses and consumers alike are still navigating how to approach these provisions.[125] State attorneys general will

---

119. Id.

120. Shannon Yavorsky & Christina Lee, New State Privacy Laws Zero in on AI, JD Supra (Aug. 12, 2022), https://www.jdsupra.com/legalnews/new-state-privacy-laws-zero-in-on-ai-7686269 [https://perma.cc/TG77-2MT6] (quoting Cal. Civ. Code § 1798.140(z)) (misquotation in original).

121. Katelyn Ringrose, New Categories, New Rights: The CPRA's Opt-Out Provision for Sensitive Data, Int'l Ass'n of Priv. Pros. (Feb. 8, 2021), https://iapp.org/news/a/new-categories-new-rights-the-cpras-opt-out-provision-for-sensitive-data [https://perma.cc/V3KW-P96R].

122. Id.; see also supra text accompanying note 29.

123. Ringrose, supra note 121.

124. Id.

125. Ronald I. Raether & Sadia Mirza, Insight: So the CCPA Is Ambiguous—Now What?, Bloomberg L. (June 14, 2019), https://news.bloomberglaw.com/privacy-and-data-security/insight-so-the-ccpa-is-ambiguous-now-what (on file with the *Columbia Law Review*) (describing how "[o]rganizations seeking to comply with the new privacy law are left in the dark trying to understand not only the intent behind certain CCPA provisions, but also how to comply").

be in charge of enforcement, and both additional privacy regulations and future litigation may help to clarify the significance and application of these provisions.[126]

Here too, this may perpetuate the skew of parties opted in versus opted out of these privacy sales, sharing, or use schemes. One such way is by litigation itself. When a business collects or shares data in a way that a consumer-turned-plaintiff feels is violative of their right to opt out, they may bring litigation against the business to seek their desired remedy. Those who understand privacy regulations enough to notice a breach of their rights are more likely to be found in the digitally literate group who would otherwise have been, and would have exercised, that opt-out right.[127] Thus, this may return to the initial problem of skewing the opt-in and opt-out populations in an unrepresentative or potentially even discriminatory way.

3. *Business Maneuvers.* — Businesses have an incentive to seek out ways around the opt-out provisions found in privacy regulations like the CCPA, the CPA, the CPRA, and the BIPA.[128] In doing so, businesses may find loopholes in the privacy regulations as they currently stand that directly counteract their purpose.

One such area is through the ambiguous language outlined above.[129] Businesses may choose to loosely configure the "reasonably related" language to be favorable to their maintenance of consumer data. Although the business has the burden of providing and justifying the calculus for understanding this relatedness, businesses can construct the relatedness in a way that both suits them and is acceptable under the state privacy acts.

Additionally, the other problematic possibility is that businesses may use an individual's *lack* of opt-out as its own category to use for targeted ads or information collection. It is probable, given the overlap between those who do not opt out and those who fall prey to dark patterns because of that group's lack of digital literacy,[130] that businesses will double down on the populations who do not opt out.[131] Given that these populations have chosen not to opt out and may also lack the media literacy to recognize deceitful consumer practices, they are increasingly at the mercy of the way those businesses choose to use their sensitive, biometric, and personal information.

---

126. See, e.g., Cal. Civ. Code § 1798.199.90 (2023) (giving the state Attorney General the power to enforce the CCPA); Colo. Rev. Stat. § 6-1-1331 (2023) (same); Va. Code Ann. § 59.1-584 (2023) (same).

127. See supra section II.A.

128. See supra notes 88–89 and accompanying text.

129. See supra section II.B.2.

130. See supra section II.A.

131. See supra note 104 and accompanying text.

Finally, a tactic that businesses may use to avoid privacy regulations impacting their bottom line is to ignore them altogether. As it stands, most privacy regulations, in large part because of their newness, contain a cure period to allow for a business to remediate any violations they make and come in line with the regulation.[132] In the Sephora case, the company was given a thirty-day warning period that they were in violation of the CCPA, and instead of working to repair the situation, they ignored the notice entirely.[133] Companies have been aware of the CCPA since 2018, yet "many brushed it off, believing it either wouldn't apply to them, hurt their checkbooks, or affect how consumers felt about their brands."[134] The Sephora settlement may serve as a wake-up call to many businesses, realizing that law enforcement made "clear [they would] not hesitate to enforce the law," that "[t]he kid gloves are coming off," and that businesses must either get with the program or face the consequences.[135] That said, newer regulations like the CPA did not undergo enforcement until July 2023.[136] Given this piecemeal enforcement, there is still a chance that businesses will choose to continue their violative practices for as long as they can get away with them before either litigation or enforcement periods come to pass.

III. ROOM FOR REMEDY

The online privacy space, while still constantly developing, runs the risk of being a force for discrimination and harmful practices. Privacy regulations are costing businesses money, and these companies can continue or find new ways to exploit vulnerable populations that may not have the requisite digital literacy to be able to avoid the traps, such as confusingly designed opt-out sections on their webpages. This Part proposes ways to limit the harm that is caused as the privacy landscape continues to evolve and change through moving towards an "opt-in" system, passing federal privacy regulation, or redesigning and orienting the way that opt-out provisions are presented to consumers.

---

132. See, e.g., Data Privacy FAQ's: How Do Cure Periods Work Under the New State Privacy Laws?, Bryan Cave Leighton Paisner LLP (Aug. 24, 2022), https://www.bclplaw.com/en-US/insights/data-privacy-faqs-how-do-cure-periods-work-under-the-new-state-privacy-laws.html [https://perma.cc/343B-WUZ2]. The privacy laws of Colorado, Connecticut, Utah, and Virginia contain cure periods. The California law does not, although it does give the enforcement agency discretion in allowing a cure period. Id.

133. Chavez, supra note 65 (discussing "the 30-day warning period given to companies to fix their privacy violations—something California said Sephora received and ignored").

134. Id.

135. Id. (internal quotation marks omitted) (quoting California Attorney General Rob Bonta).

136. See 2021 Colo. Sess. Laws 3445; Colorado Privacy Act (CPA), supra note 58.

A. *Changing "Opt-Out" to "Opt-In"*

The General Data Protection Regulation (GDPR) is the European Union's comprehensive data privacy law,[137] and instead of the "opt-out" regime seen in the state regulations across the United States, the GDPR uses an opt-in format for privacy and data protection.[138] The GDPR requires opting in for any use of online trackers, called "cookies," and, in most cases, also requires asking the user for consent to process their data."[139] This consent must be "given freely, specific, informed, and unambiguous. Otherwise, it doesn't count as an opt-in."[140] The opt-in approach is also used by Brazil's and Thailand's data privacy regulations, demonstrating international acceptance of a framework the United States has not embraced.[141]

Under the GDPR, "a lawful ground is needed for collecting or using any personal data (under Article 6) and where collecting or using sensitive personal information is generally prohibited as a rule (under Article 9(1))."[142] Further, for a business to be permitted to access sensitive personal information, "a specific permission listed under Article 9(2) must be applicable, such as explicit opt-in consent, providing medical services, or for scientific research purposes, only as long as necessity and proportionality conditions are met."[143]

Considering that much of the current skewed representation of those who do not opt out versus those who do is due to lack of knowledge, awareness, or ability to navigate the options to be able to opt out,[144] an opt-in regime would largely remedy this issue. Instead of the default being data sharing or selling, the default would be the refusal of that, with an option to participate if desired. If this solution were adopted on a national scale, it would play a huge role in flipping a discriminatory aspect of the existing laws.

There are arguments that an opt-in privacy system would not offer additional protections for consumers. Although consumers would be

---

137. See Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1, 32 ("This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.").

138. The Difference Between Opt-In vs Opt-Out Principles in Data Privacy: What You Need to Know, Secure Priv., https://secureprivacy.ai/blog/difference-beween-opt-in-and-opt-out [https://perma.cc/4AA3-FLRZ] [hereinafter Opt-In vs Opt-Out Principles in Data Privacy] (last visited Oct. 29, 2023).

139. Id.

140. Id.

141. Id.

142. Ringrose, supra note 121.

143. Id.

144. See supra notes 97–103 and accompanying text.

required to "accept" or "agree" to their data collection, much of the language informing consumers of their rights and the ways the data would be used is lengthy, averaging more than 2,500 words and "carefully drafted to maximize data use and minimize legal exposure."[145] As a result, "[f]ew consumers read these policies before agreeing to give up information, and the practices of ad networks and social media are not clear to most [consumers] when [they] click the 'I agree' button."[146] Even though the opt-in system would permit consumers to opt in, many people may be ignorant, or even indifferent, as to what they are agreeing to, so having an opt-in provision versus an opt-out would have little positive impact.[147]

But regardless of whether people are aware when they choose to opt in, proactively presenting the option to opt in requires an affirmative step to allow a business to collect personal information. This requirement alone may give pause, and as seen with the Apple iOS feature, many will take advantage of the ability to decide outright not to have their data collected, shared, or sold.[148] This forced decision may allow for the less digitally literate to find a way out of being one of the primary demographics left with their data traded by businesses without their understanding.

B. *Implementation of a Federal Data Privacy Law*

Another potential solution, perhaps implemented in conjunction with an opt-in system, is for the United States to implement its first comprehensive national data privacy law. Currently, no data or biometric privacy protection exists at the federal level, as the National Biometric Information Privacy Act proposed by Senators Jeff Merkley and Bernie Sanders in 2020 has since died.[149] In the meantime, state-specific biometric privacy information regulation governs. Although the patchwork system in place has had a ripple effect, spreading the implementation of data privacy laws across the states, it has been done individually, and the regulations are not always in agreement.[150] As it stands presently, "a complex state

145. Peter M. Lefkowitz, Opinion, Why America Needs a Thoughtful Federal Privacy Law, N.Y. Times (June 25, 2019), https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html (on file with the *Columbia Law Review*).

146. Id.

147. See id.

148. See supra note 105–107 and accompanying text.

149. S. 4400 (116th): National Biometric Privacy Act of 2020, GovTrack, https://www.govtrack.us/congress/bills/116/s4400 [https://perma.cc/ZD4G-5D2B] (last visited Dec. 28, 2022) (showing no vote on this bill).

150. Daniel Castro, Luke Dascoli & Gillian Diebold, Info. Tech. & Innovation Found., The Looming Cost of a Patchwork of State Privacy Laws 1 (2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws [https://perma.cc/226P-FL7T] ("Congress should pass federal privacy legislation that preempts states, protects consumers, and promotes innovation.").

privacy patchwork of 50 laws could cost companies over $1 trillion—and $200 billion for small businesses."[151] Privacy legislation functioning as independent, overlapping units instead of as a cohesive system could critically impact the United States, especially in competing in a global market, in which regulations like the GDPR provide comprehensive and inclusive systems of privacy regulation elsewhere.[152] By contrast, in the United States, businesses are forced to navigate and be aware of multiple state privacy regulations and be prepared to face repercussions from any of them. This system can be confusing and muddled.[153]

The FTC says that it has brought "hundreds of enforcement actions against companies over the last two decades for violations of privacy and data security."[154] Among these violations were unauthorized sharing and selling of sensitive personal information and inadequate protections of personal data.[155] Despite the enforcement actions the FTC has brought, the agency recognizes that its impact and ability to "deter illegal conduct is limited because it generally lacks authority to seek financial penalties for initial violations of law. That could change if the comprehensive privacy legislation were to clear Congress."[156] With a federal data privacy law, enforcement could come from the federal level instead of exclusively the state level. The ability for businesses to circumvent violations and perpetuate discriminatory practices could be diminished if they were exposed to additional, and perhaps more serious, ramifications from additional sources.

Yet, if a federal data privacy law is enacted, as may happen with the American Data Privacy Protection Act (ADPPA),[157] questions of effectiveness, preemption, and timeline for both enactment and enforcement arise.[158] For one, the ADPPA would preempt "the majority of state or local

151. Jordan Crenshaw, It's Time to Get Serious About National Data Privacy Legislation, U.S. Chamber of Com. (Jan. 28, 2022), https://www.uschamber.com/technology/data-privacy/its-time-to-get-serious-about-national-privacy-legislation [https://perma.cc/CHS4-WTS7] (citing Castro et al., supra note 148).

152. See Castro et al., supra note 150, at 1.

153. See supra note 43 and accompanying text.

154. Marcy Gordon, FTC Considers Regulating How Tech Companies Collect Your Data, WUSA9 (Aug. 11, 2022), https://www.wusa9.com/article/news/nation-world/ftc-considers-limiting-tech-data-collection/507-680349d7-a106-4af6-90b4-474fbb55f1a7 [https://perma.cc/3URT-92X8].

155. Id.

156. Id.

157. See American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

158. Emily Catron & Gary Kibel, Federal Data Privacy Legislation: Differences With State Laws Raise Preemption Issues, Reuters (Aug. 10, 2022), https://www.reuters.com/legal/legalindustry/federal-data-privacy-legislation-differences-with-state-laws-raise-preemption-2022-08-10 [https://perma.cc/NU9H-BQZG].

laws, invalidating any similar provisions enacted under state law."[159] State laws like the BIPA would not be preempted by the ADPPA, however.[160] The result of this "strange preemption landscape is a continuation of the patchwork of multiple, non-comprehensive privacy and data protection laws that exists today. For example, many businesses would need to separately comply with the differing requirements of the ADPPA and certain state privacy laws."[161] Finally, in regard to enforcement, the ADPPA would be enforceable by state attorneys general, the FTC, private authorities, and private citizens, though private rights of action would be prohibited in the first two years of its enactment.[162] This enforcement scheme would extend the amount of time before individuals could pursue their own litigation and could mean fewer repercussions for violators in that time period. Under this framework, a possibility still exists that this unified Privacy Act would allow for opt-out provisions to persist and for the existing system to continue in much the same way it presently functions. The populations made most vulnerable by the existing provisions may remain exactly that: vulnerable.

An additional counterargument to having a federal data privacy law is that having "rigid rules about the 'sale of data' and limits on the use of artificial intelligence are not a productive way to prevent abuse and would impact activities essential to our safety and security."[163] To some degree, the sharing of data can assist with "essential activities—including advances in health care, cybersecurity, financial services and fundamental scientific research [which] depend upon large data sets and broad data sharing."[164] Although sharing large amounts of data may assist with matters such as health research, the dangers inherent in giving individual personal information to algorithms and businesses is incredibly high, especially in communities of color.[165]

Despite these counterarguments, implementation of a federal data privacy law could still offer significant protections to consumers, especially those from less-digitally-literate populations. A uniform data privacy law would allow for there to be a more robust list and understanding of the "do's" and "do not's" and a more predictable and consistent means of enforcement. Whereas now the patchwork system allows for businesses to find loopholes and exploit the newness and ambiguity therein, a federally

---

159. Id.

160. Id. ("[T]he ADPPA does not preempt all state privacy laws, such as the Illinois Biometric Information Privacy Act (BIPA).").

161. Id.

162. Id.

163. Lefkowitz, supra note 145.

164. Id.

165. See supra notes 5–7 and accompanying text.

implemented and strictly enforced regulation would help to clarify expectations and potentially remove some of the systematic manipulation. There is also a likelihood the United States would mimic the GDPR to take advantage of an existing framework spanning multiple countries and regions, which would also potentially mean use of the opt-in versus opt-out system. Further, it would be easier for rights organizations to disperse resources and inform the public of their rights on a national scale, rather than catering to fifty different privacy schemes, thus improving digital literacy and empowering consumers at risk of being targeted by businesses preying on those who do not opt out.

C. *Adjusting the Opt-Out Website Options*

Reformatting the way that websites and businesses present their opt-out options may benefit consumers by granting them tools to make an informed decision in the existing opt-out system. At present, the CCPA, the CPRA, and the CPA all require an obvious and apparent placement of the opt-out option on the webpage.[166] Further, as in the GDPR, entering a website triggers a pop-up that asks visitors if they consent to data collection, sharing, or selling.[167] Those populations who are digitally literate have a higher correlation with finding the aforementioned "opt-out" option and choosing to opt out.[168]

Additionally, as seen with the Apple example, when populations were given an explicit "opt-out" choice, ninety-six percent chose to opt out.[169] Presenting the opt-out option in the same manner that the opt-in has been presented could be beneficial by providing a means for those who are not as digitally literate to still establish whether they would like their data to be collected, shared, or sold. Upon entering a website, a consumer would encounter a pop-up button that would ask if they would like to opt out of data collection, sale, or sharing. While some businesses may already do this, making this pop-up a standard practice and a uniform style across the board could offer more vulnerable populations a fairer opportunity to take control of their data and information.

Including this language in the next wave of privacy regulation would allow for even greater transparency and perhaps an opportunity to avoid the racialized skew resultant from a digital literacy divide.

---

166. See supra section I.C.2.

167. Opt-In and Opt-Out Principles vs Data Privacy, supra note 138.

168. See supra section II.A.

169. Axon, supra note 106.

CONCLUSION

The world of privacy and data privacy regulation is here to stay. As the laws develop and states produce new and more comprehensive versions of the regulations that came before them, it is increasingly apparent that questions about discrimination and bias in algorithms and data collection processes will persist, and rightly so. As it stands, there is space for businesses to use loopholes and ambiguities in the regulations to sidestep the mandates, perpetuating a discriminatory system in the process. The CCPA, the CPRA, the CPA, and the BIPA are all representative of the state of privacy regulation and the way that regulations may continue to evolve as time continues. As additional regulations do come about, moving to an opt-in system, creating federal data privacy legislation, or changing the appearance of the opt-out option may help to avoid the perpetuation of problematic business practices that these regulations have permitted in the consumer data privacy space. Privacy rights are more protected than they once were, but "[p]rogress looks like not completely perfect laws; there is no such thing. It looks like fits and starts."[170]

170. Shira Ovide, The Messy Progress on Data Privacy, N.Y. Times (May 12, 2022), https://www.nytimes.com/2022/05/12/technology/federal-data-privacy-law.html (on file with the *Columbia Law Review*) (last updated May 15, 2022).