Roger Williams University Law Review

Volume 27
Issue 3 *Vol 27, Iss. 3 (Summer 2022)*

Article 5

Summer 2022

The Wild West of Data Privacy: Why Rhode Island Needs to Enact Comprehensive Legislation to Protect Consumers' Data

Candace Quinn
Candidate for Juris Doctor, Roger Williams University School of Law

The Wild West of Data Privacy: Why Rhode Island Needs to Enact Comprehensive Legislation to Protect Consumers' Data

Candace Quinn*

INTRODUCTION

"The Party seeks power entirely for its own sake. We are not interested in the good of others; we are interested solely in power–pure power."[1] In George Orwell's acclaimed novel, *1984*, the Party controlled citizens through constant, pervasive surveillance.[2] Any group, organization, or enterprise that gathers continuous information from a large swath of people possesses inordinate power over said people. This phenomenon became a reality through big data where large technology companies gather massive amounts of personal information from individuals' phones, computers, and Amazon Alexas without their knowledge and absent informed consent.[3] This unmitigated power challenges the vital right of privacy that all Americans must be able to enjoy.

---

* Candidate for Juris Doctor, Roger Williams University School of Law, 2023. I would like to thank my editors, Sam Ferrucci and Amanda Reis, for their invaluable guidance. I want to thank my family for their unyielding support and encouragement and Professor Margulies for his helpful feedback.

1. GEORGE ORWELL, 1984 (1949).
2. *See id.*
3. *See* Michael McFarland, *Unauthorized Transmission and Use of Personal Data*, SANTA CLARA UNIV. (June 1, 2012), https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unauthorized-transmission-and-use-of-personal-data/ [https://perma.cc/3D96-KQDV].

This Comment analyzes data privacy in Rhode Island and suggests that Rhode Island adopt a data privacy law analogous to California's comprehensive statute. Most consumers are unaware of how companies and other actors gather and profit off their personal information.[4] To address this problem, this Comment examines the patchwork of federal and state laws concerning data privacy in the consumer context.[5] This Comment illustrates how the California Privacy Rights Act protects consumers' data by giving consumers the right to opt out of the sale of their personal information, the right to know what information has been collected and the right to access personal information, the right to delete their information, the right to limit use and disclosure of sensitive personal information, and the right to correct inaccurate personal information.[6]

In contrast to California, and a few other states, Rhode Island lacks a data privacy law altogether.[7] Rhode Island should act to protect consumers' personal information by enacting a data privacy law incorporating many elements of California's comprehensive statute. A suitable data privacy law is vital in precluding private businesses and third parties from profiting off users' data without consumers' informed consent, providing consumers with control over their personal information, and enabling consumers to determine whether to share their personal information.[8]

Part I of this Comment explores the history of the right to privacy in America, the ways through which companies gather consumers' personal information and garner profits, and how data brokers employ consumers' personal information.[9] Part II analyzes existing federal law on data privacy and why it remains insufficient

---

4. *See id*.

5. Steven C. Bennett, *The "Right to be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 168 (2012).

6. *See generally* CAL CIV. CODE §§ 1798.105–.106, .110, .120–.121 (West 2022).

7. At the time of publishing, Virginia and Colorado have also passed comprehensive data privacy statutes. Mary J. Hildebrand, *U.S. Privacy 2022: Compare, Contrast, and Integrate New State Laws*, LOWENSTEIN SANDLER LLP (Dec. 9, 2021), https://www.lowenstein.com/news-insights/publications/articles/us-privacy-2022-compare-contrast-and-integrate-new-state-laws-mary-hildebrand [https://perma.cc/LN84-8MTY].

8. *See* McFarland, *supra* note 3.

9. While a significant portion of this Comment focuses on data brokers, it is important to note that data brokers are only one aspect of data privacy.

to protect consumers. Subsequently, Part II introduces the California Consumer Privacy Act and the recently passed California Privacy Rights Act examining their significant additions to data privacy in the United States. Consequently, Part II contrasts California's legislation with proposed data privacy legislation in Rhode Island. Part III evaluates how specific rights afforded to California consumers through the California Privacy Rights Act provide consumers autonomy and control over their data and argues why Rhode Island should adopt many of the same measures. Finally, Part IV addresses multiple counterarguments against Rhode Island adopting a comprehensive data privacy statute finding that they lack merit and concludes with legislative recommendations for the state.

I. THE INCEPTION OF DATA PRIVACY

The right to privacy in America developed alongside the common law.[10] Justice Brandeis and Justice Warren brought privacy issues to the forefront in their law review note examining "the right to be let alone."[11] Specifically, the Justices recognized the damage that results from a violation of privacy.[12] "[M]odern enterprise and invention have, through invasion upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[13] The Justices emphasized how technology had chipped away at individuals' privacy.[14] Moreover, they compared a privacy claim to that of libel or slander, noting their distinct similarities in mental damage to a person rather than physical injury.[15] This note set the stage for privacy discourse in America for years to come.[16]

10. Any reference to the Fourth Amendment is outside the scope and will not be included in this Comment.

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

12. *Id.* at 196.

13. *Id.*

14. FREDERICK S. LANE, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 62 (2009).

15. Warren & Brandeis, *supra* note 11, at 197.

16. LANE, *supra* note 14, at 61–62.

By 1967, thirty-five states acknowledged a right to privacy through the common law or by statute.[17] Rhode Island and Nebraska were the only remaining states without a discrete right to privacy by 1975.[18] In 1980, Rhode Island passed the Right to Privacy statute which incorporated, "[t]he right to be secure from unreasonable intrusion upon one's physical solitude or seclusion; [t]he right to be secure from an appropriation of one's name or likeness."[19] The statute created a cause of action for an invasion of the right to privacy which reflected the states growing awareness of its importance.[20]

A. *Data Privacy and the Role of Data Brokers*

Data privacy is defined as "the ability of a person to determine for themselves when, how and to what extent personal information about them is shared with or communicated to others."[21] Private businesses gather a myriad of information from consumers' online activity.[22] Certainly, companies gather what information consumers directly provide to them: their name, phone number, and email.[23] Search engines are particularly powerful in this domain because they collect huge amounts of data on a single consumer through frequency of use.[24] Engagement data includes how a consumer interacts with the company including what features they use, and companies track the consumers' location.[25] Additionally, social media sites, such as Meta and Instagram, collect information

17. Time, Inc. v. Hill, 385 U.S. 374, 413 (1967) (Fortas, J., dissenting); Memorandum from Sally Pfieffer, Am. Civ. Liberties Union of R.I., to Betsy Grossman 1, 2 (Jan. 29, 1975).

18. Pfeiffer, *supra* note 17, at 3.

19. R.I. GEN. LAWS § 9-1-28.1 (2022).

20. Pfeiffer, *supra* note 17, at 1–3.

21. *What is Data Privacy?*, CLOUDFLARE, https://www.cloudflare.com/learning/privacy/what-is-data-privacy/ [https://perma.cc/DF5A-BCK9] (last visited Dec. 23, 2021).

22. *See* McFarland, *supra* note 3.

23. *Id.*

24. *Id.*

25. Max Freedman, *How Businesses are Collecting Your Personal Data (And What They're Doing with It)*, BUS. NEWS DAILY (June 17, 2020), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/42GG-EAVF].

by examining individuals' posts, likes, and shares.[26] Meta permits consumers to examine the social media sites selected preferences for them on their "ad preferences" page; the traits listed on this page include political leanings and affinity with a specific racial or ethnic group.[27] Companies also examine consumers' purchases and related searches for products to deduce their family size, relationship status, gender, and interests.[28] These examples merely illustrate a few of the many ways that companies gather consumer data.

Massive technology companies employ swaths of data to increase profits in multiple ways.[29] "Big data" is defined as "extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations."[30] Data analytics and artificial intelligence transform these data sets into useful marketing materials.[31] Companies take those recommendations and apply them to suggest ads for the consumer; all of this information gathering about a consumers' interests and lifestyle results in tailored ads for each consumer.[32] "In the online commercial world, consumer data is both an input for other online services and a commodity asset for advertisers."[33]

Data brokers remain a largely invisible player to the general public and their business model relies solely on gathering information about consumers, repackaging it, and selling it.[34] These

---

26. Paul Hitlin et al., *Facebook Algorithms and Personal Data*, PEW RSCH. CTR. (Jan. 16, 2019), https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/ [https://perma.cc/6HY8-8YXT].

27. *Id.*

28. McFarland, *supra* note 3.

29. *See id.*; FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 1, 11 (2014), Another common way that technology companies profit off consumers' personal information is by selling it to data brokers. *Id.* at 13–14.

30. *What is Unstructured Data?,* FUEL CYCLE, https://fuelcycle.com/blog/what-is-unstructured-data/ [https://perma.cc/Z63B-458Y] (last visited Nov. 3, 2021).

31. Freedman, *supra* note 25.

32. McFarland, *supra* note 3.

33. Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 131 (2015).

34. *Id.* at 131–32. Data brokers are defined as, "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an

companies obtain information through multiple means, but the focus of this Comment will be data brokers purchasing of data from online sources.[35] These companies gather and store information on nearly every United States household, and employ this data to determine characteristics about an individual or household.[36] Further, some data brokers store consumers' personal information indefinitely.[37] An intricate part of data brokers' business model includes selling consumers' personal information to other data brokers; how far consumers' personal information travels from its initial entry point is unclear.[38] In Rhode Island, consumers possess no recourse to obtain their information from data brokers or prevent the data collection in the first place.[39] A report from the Federal Trade Commission (FTC) about data brokers included a series of legislative recommendations; many of which California adopted in its comprehensive statute.[40] Consumers in Rhode Island should be similarly shielded from data brokers benefitting from their personal information without their knowledge or informed consent.

The mass data collection by private technology companies and other private entities is deeply troubling.[41] Not only are most consumers largely unaware of the practice, but consumers in Rhode Island are unable to stop this information gathering and selling.[42] Presently, individuals rely on the internet more than ever, and these data privacy issues will only become more apparent as time passes. Thus, Rhode Islanders deserve decisive, robust legislation to protect consumers' right to privacy and permit consumers to maintain control over their personal information online.

---

individual's identity, or detecting fraud." FED. TRADE COMM'N, *supra* note 29, at 3.

35. FED. TRADE COMM'N, *supra* note 29, at 13.

36. *Id.* at 46–47.

37. *Id.* at 48.

38. *Id.* at 14.

39. Rhode Island has failed to enact any laws that contain protections for consumers from data brokers. At the time of publication, the Data Elimination and Limiting Extensive Tracking and Exchange Act (DELETE) has been introduced, in Congress, which would allow consumers to submit a request to delete all personal information to data brokers. H.R. 6752, 117th Cong. (2022).

40. FED. TRADE COMM'N, *supra* note 29, at 50. *See generally* CAL CIV. CODE §§ 1798.105–.106, .110, .120–.121 (West 2022).

41. *See* McFarland, *supra* note 3.

42. *See id.*

II. THE DATA PRIVACY LEGAL LANDSCAPE

Congress has not passed a comprehensive data privacy statute.[43] Instead, current federal data privacy laws address specific sectors or groups.[44] For example, Congress passed the Children's Online Privacy Protection Act (COPPA) which protects the personal information of children who are ages twelve and under.[45] The FTC has the authority to regulate privacy within consumer protection under Section Five of the Federal Trade Commission Act governing "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[46] The 1980 Unfairness Statement by the FTC further defined the requirements for an unfair, actionable, consumer injury including violations of privacy rights, specifying that "[the injury] must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided."[47] The FTC's interpretation of the FTC Act through the Unfairness Test, specifically the first prong involving substantial harm, protects consumer privacy rights.[48] Relying on Section Five of the FTC Act, the FTC also looks at deception in determining if a consumer injury resulted; "the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[49] The FTC possesses some practical enforcement authority that it exercises, but the FTC Act suffers from a number of shortcomings.

---

43. Blaire Rose, *The Commodification of Personal Data and the Road to Consumer Autonomy Through the CCPA,* 15 BROOK. J. CORP. FIN. & COM. L. 521, 522 (2021).

44. *See id.*

45. ANDREW B. SERWIN ET AL., PRIVACY, SECURITY, AND INFORMATION MANAGEMENT: AN OVERVIEW 35 (2011); 15 U.S.C. §§ 6501–6506.

46. 15 U.S.C. § 45.

47. *FTC Policy Statement on Unfairness*, FED TRADE COMM'N (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/7XER-EJ4C]; Ohlhausen & Okuliar, *supra* note 33, at 146–47.

48. Ohlhausen & Okuliar, *supra* note 33, at 147.

49. *See FTC Policy Statement on Deception*, FED TRADE COMM'N (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/KF7C-BA4P].

The FTC's enforcement authority remains limited in some areas. Namely, Section Five does not permit the FTC to pursue civil penalties for initial infractions.[50] The FTC obtains rulemaking authority for Congressional statutes like COPPA; however, the FTC does not obtain rulemaking authority for general privacy concerns.[51] Furthermore, Section Five of the of the FTC Act does not apply to non-profits and common carriers, thereby shielding them from the FTC's authority.[52] Within a report titled *FTC's Use of Its Authorities to Protect Consumer Privacy and Security*, the FTC recommended that Congress pass a statute to address these shortcomings.[53] Consequently, this reinforces the necessity of a comprehensive data privacy statute in Rhode Island given the inadequate protections provided by federal law and the FTC's limited enforcement capacity.

A. *Comparing Rhode Island and California's Data Privacy Laws*

In 2018, the California legislature passed the California Consumer Privacy Act (CCPA) which went into effect in 2020.[54] Many legal scholars consider this statute groundbreaking within the United States, because of the broad protection it provides for consumers.[55] Under this law, California residents may request that a business that collected their personal information permanently

---

50. FED. TRADE COMM'N, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY 4 (2020).

51. *Id.* at 7.

52. *Id.* at 8.

53. *Id.*

54. Kari Paul, *California's Groundbreaking Privacy Law Takes Effect in January. What Does it Do*?, GUARDIAN (Dec. 30, 2019), https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do [https://perma.cc/22SX-2VEZ].

55. *Id.* (The author referred to this legislation "as giving residents unprecedented right to control what information companies collect on them and how it is used"); Issie Lepowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ [https://perma.cc/6EVA-GPMK] (The article emphasized how the legislation would "set the standard for states across the country."). *See generally* David A. Zetoony, *The Desk Reference Companion to the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act*, AM. BAR ASS'N, https://www.americanbar.org/products/inv/book/415169229/ [https://perma.cc/RCA5-UQ9P] (last visited Feb. 21, 2022).

delete the data.[56] Additionally, if a business sold a consumers' personal information to third parties, then the consumer can "opt out" by instructing businesses to cease selling their personal information to third parties.[57] The statute enables consumers to request businesses that collected their personal information to provide, to the consumer, what personal information they gathered, what type of information they gathered, and how the company is using it.[58] The CCPA may have caused technology companies to lose out on profit streams that they reliably received prior to its enactment and incentivize these companies to stop serving California residents in the same manner.[59] The right of no retaliation combats this problem by forbidding businesses from discriminating against California consumers for utilizing any of these rights.[60] These are some notable provisions of the CCPA that provide considerable privacy to consumers.

California passed the California Privacy Rights Act (CPRA) in 2020, due to become operative in 2023, which incorporates all the critical portions of the CCPA and contains a few additions.[61] This revised data privacy statute was a ballot initiative known as Proposition Twenty-Four.[62] The CPRA will establish the California Privacy Protection Agency (Agency), the first of its kind, to enforce the statute.[63] "The agency shall be governed by a five-member board, including the chairperson."[64] The CPRA contains the requirements and qualifications for the board members;[65] the Agency obtains

56. CAL. CIV. CODE § 1798.105 (West 2022).

57. CAL. CIV. CODE § 1798.120 (West 2022).

58. CAL. CIV. CODE § 1798.110 (West 2022).

59. Companies must pay for compliance costs as well. *See* Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion to Get into Compliance*, CNBC (Oct. 5, 2019), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html [https://perma.cc/Z27Q-FJAF].

60. CAL. CIV. CODE § 1798.125 (West 2022).

61. *California Privacy Rights Act: An Overview*, PRIV. RTS. CLEARINGHOUSE (Dec. 10, 2020), https://privacyrights.org/resources/california-privacy-rights-act-overview [https://perma.cc/F97E-CYA8].

62. *Id.*

63. CAL. CIV. CODE § 1798.199.10 (West 2022).

64. *Id.*

65. CAL. CIV. CODE § 1798.199.15 (West 2022).

rulemaking authority.[66] The additions contained in the CPRA support necessary enforcement authority for this broad statute.

The CPRA also includes some substantive additions; one such inclusion permits consumers to request businesses correct faulty personal information collected about them, requiring businesses to "use commercially reasonable efforts to correct the inaccurate personal information."[67] Additionally, the "Consumers' Rights to Limit Use and Disclosure of Sensitive Personal Information" allows consumers to instruct a business that collects their sensitive personal information to limit the use to strictly its service or function.[68] This Comment focuses on the CPRA as it subsumes the CCPA.

Rhode Island law contains no specific statute to protect consumers' personal information online. However, there are several proposed statutes making their way through the legislature that tackle various data privacy issues. One proposal aims to limit the ability of social media companies to "use, gather, capture, quantify or sell any consumer internet data for profit, without the consent of, and payment of compensation to, the consumer generating such data."[69] The proposed Rhode Island Transparency and Privacy Protection Act (the Act) requires websites to notify consumers of any third parties to whom the website may disclose consumers' personally identifiable information.[70] In addition, the Act requires websites that gather consumers' personal information to "identify all categories of personal information" collected.[71] Another statute introduced in 2021 compels any business that gathers consumers' identification information to possess a data privacy policy made available to the public.[72] While each of these statutes tackle an aspect of data privacy, even viewed in their totality, many crucial protections for consumers are still absent; a broader statute resembling the CPRA presents a better overall solution.

66. CAL. CIV. CODE § 1798.199.40 (West 2022).
67. CAL. CIV. CODE § 1798.106 (West 2022).
68. CAL. CIV. CODE § 1798.121 (West 2022).
69. H.B. 5509, 2021 Leg. Sess. (R.I. 2021).
70. *Id.*
71. *Id.*
72. H.B. 5513, 2021 Leg. Sess. (R.I. 2021).

III. THE CALIFORNIA PRIVACY RIGHTS ACT ENABLES CONSUMERS TO PREVENT COMPANIES FROM PROFITING OFF THEIR DATA

Companies gathering and subsequently profiting off consumers' data is not inherently problematic or immoral.[73] If consumers were cognizant of how companies earned money from their data and offered informed consent for companies to use their data in that manner, than this practice presents no ethical issue.[74] Unfortunately, technology companies' data collection, aggregation, and profit from consumers' data takes place without consumers' knowledge often resulting in exploitation.[75] Rhode Island's utter lack of enacted data privacy legislation leaves consumers vulnerable to these continued profit streams to internet companies and third parties at the consumers' expense.[76]

For instance, when someone owns the Amazon voice assistant, Alexa, it sits in an individual's home and inputs all the sounds in the vicinity, including an infant crying, a dog barking, and any conversation that takes place.[77] This device gains access to the most personal aspects of someone's life.[78] Amazon turns around and employs that data for advertising recommendations and shares the information with third parties.[79] In Rhode Island, technology conglomerates remain unimpeded in how they manage consumers' data for the company's benefit often opting to store the big data permanently.[80] The right to delete and the right to require businesses to stop selling or sharing a consumers' personal information both stop this vicious cycle of technology companies taking advantage of defenseless consumers for their own financial gain.[81]

---

73. *See* McFarland, *supra* note 3.

74. *See id.*

75. *See id.*

76. *See id*.

77. *See* Lauren Bass, *The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age of Alexa*, 30 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 261, 273 (2019).

78. *Id.* at 274–75.

79. *See* Andrew Williams, *Smart Home Privacy: What Amazon, Google and Apple Do with Your Data,* AMBIENT (Jan. 21, 2022), https://www.the-ambient.com/features/how-amazon-google-apple-use-smart-speaker-data-2765 [https://perma.cc/BGP4-MJ36].

80. *See id.*; Bass, *supra* note 77, at 280.

81. CAL. CIV. CODE §§ 1798.105(a), .120(a) (West 2022).

The right to delete is arguably the most impactful of all the new rights contained in the CPRA.[82] The European Union called this the "right to be forgotten" which gives consumers the ability to "have their data fully removed when it is no longer needed for the purposes for which it was collected."[83] The CPRA's iteration of the right to delete states: "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected."[84] This right does contain a number of exceptions for businesses that receive a verified request.[85] Businesses are excepted if they collect the personal information for certain purposes: as part of a product recall; to protect the consumers' right of free speech; to troubleshoot any errors; to aid in "peer-reviewed scientific, historical, or statistical research;" or for internal uses that line up with consumer anticipation.[86] This right places the power back in the hands of consumers to determine if they want a company to retain their personal data.[87] Therefore, the right to delete provides a crucial opportunity for consumers to halt the cyclical profiting process by completely removing their information from the company's domain.[88]

A. *Restricting Data Broker and Third-Party Profits*

The CPRA broadly defines third parties that buy and collect consumers' information in an exclusionary fashion as any company that does not directly gather the personal information from the consumer or a "person to whom the business discloses consumers' personal information for a business purpose pursuant to a written contract."[89] An expansive definition is fitting given the breadth of the technology industry that collects consumer information outside of sites that consumers directly visit. Third parties, such as data

82. § 1798.105(a).

83. *Memo of the European Commission on Data Protection Reform – Frequently Asked Questions*, EUROPEAN COMM'N (Nov. 2, 2010), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_10_542 [https://perma.cc/9DSP-N4SB].

84. § 1798.105(a).

85. CAL. CIV. CODE § 1798.105(d) (West 2022).

86. *Id.*

87. CAL. CIV. CODE § 1798.105(c)(1) (West 2022); *see* Williams, *supra* note 79.

88. CAL. CIV. CODE §§ 1798.105(c)(1), (c)(3) (West 2022).

89. CAL. CIV. CODE §§ 1798.140(j)(1), (ai) (West 2022).

brokers, present a serious threat to consumer privacy because of the largely unseen accumulation of consumers' personal information.

The "Consumers Right to Opt-Out of [the] Sale of Personal Information" averts third parties profiting off the spread of consumers' personal information without the consumers' knowledge or informed consent.[90] If consumers exercise this right, it prevents companies from selling or sharing their personal information.[91] This right intimately involves data brokers as their business model relies on the passage of information from technology companies to third parties who take their cut by selling consumers' personal information to another third party.[92] The "status quo" involves a seemingly endless redistribution of consumers' personal information that centers around each party profiting along the way, and each company holding on to consumers' data as long as they please.[93] This portion of the CPRA, if consumers choose to use it, stops the circulation of consumers information and precludes third parties from earning money from the deal.

The amended portion of the right to delete, contained in the CPRA, added a section requiring third parties to erase consumers' personal data.[94] If a consumer sent a request to delete to the company that gathered their information, the addition requires the company to contact all third parties that possess the consumer's information as well to delete it "unless this proves impossible or involves disproportionate effect."[95] This obligation applies to service providers and contractors as well.[96] Additionally, the service providers and contractors must convey the consumer's request to delete their information to any affiliated service providers and

90. CAL. CIV. CODE § 1798.120(a) (West 2022) ("A consumer shall have the right, at any time, to direct a business that sells or shares personal information about a consumer to third parties not to sell or share the consumer's personal information.") The provision also provides additional protections for children younger than sixteen by creating a general prohibition on selling or sharing children's info absent additional consent. CAL. CIV. CODE § 1798.120(c) (West 2022).

91. § 1798.120(c).

92. FED. TRADE COMM'N, *supra* note 29, at 13–14.

93. *See id.* at 14, 48.

94. CAL. CIV. CODE § 1798.105(c)(1) (West 2022).

95. CAL. CIV. CODE § 1798.105(c)(3) (West 2022).

96. *Id.*

contractors.[97] However, the consumer must submit the verified request to the business not to the service providers and contractors themselves.[98] This critical addition to the right to delete acknowledges how far consumers' personal information travels; merely granting consumers the ability to delete their information from the initial companies website remains insufficient to adequately protect consumers' privacy.[99]

IV. THE CALIFORNIA PRIVACY RIGHTS ACT GRANTS CONSUMERS AUTONOMY AND CONTROL OVER THEIR PERSONAL INFORMATION

The traditional notions of privacy intersect with individual autonomy by permitting people to make decisions about their own lives including "freedom from intrusion, whether physical…or technological."[100] The complete absence of regulation in Rhode Island, to protect consumers' information online, threatens the independence of Rhode Islanders' virtual selves.[101] Consumers lack "digital agency–the ability to own the rights to their personal data [and] manage access to that data."[102] All the information collected, stored, and shared by internet companies absent consumers informed consent demonstrates a complete lack of control on the part of the consumer.[103] Specifically, it is deeply problematic that consumers are unaware of what personal information companies collect about them. A Pew Research Center survey found that eighty-one percent of participants felt they have "very little or no control over the data companies collect."[104] To shore up data privacy,

97. *Id.*

98. *Id.*

99. FED. TRADE COMM'N, *supra* note 29, at 14.

100. Chen-Hung Chang, *New Technology, New Information Privacy: Social-Value-Oriented Information Privacy Theory*, 10 NAT'L TAIWAN U. L. REV. 127, 146 (2015).

101. *See* Michael McFarland, *Why We Care About Privacy*, SANTA CLARA UNIV. MARKKULA CTR. FOR APPLIED ETHICS (June 1, 2012), https://www.scu.edu/ethics/ [https://perma.cc/J3L9-479L] (search for "Why We Care About Privacy" in the search box in the upper-right corner).

102. 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 [https://perma.cc/2T63-4B4A].

103. Chang, *supra* note 100, at 131.

104. 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://www.pewresearch.org/internet/2019/11/15/americans-and-

individuals need autonomy online and protection from the frequent intrusion by for-profit entities. The federal government provides expanded protections for specific areas such as health information and personal data of children.[105] However, an average consumer online retains none of those protections. Certain provisions of the CPRA directly empower consumers to control the dissemination of their personal information, thereby combating this persistent problem.[106]

The CPRA allows consumers to exercise control over their data in several ways. A subsection of the CPRA titled, "Consumers' Right to Know What Personal Information is Being Collected [and] Right to Access Personal Information" allows consumers to request any business that gathers personal information to provide the type of personal information collected, the source of the personal information, the third party categories where the business disclosed the consumers data, and the exact personal information collected on that consumer.[107] Additionally, the business must disclose, "the business or commercial purpose for collecting, selling, or sharing personal information."[108] At the consumer's request, a business must also provide the sources of the personal information.[109] After a consumer exercises this right, if they decide they do not want a business to store the data already gathered on the consumer, they could submit a request to delete the already gathered data.[110] Each of these rights standing alone are not particularly impactful. By viewing these rights in their totality, the CPRA provides consumers with substantially more control over their personal information and starkly contrasts the absent protections in Rhode Island.

Two other pivotal provisions contained in the CPRA include the right to correct faulty information and additional protections for sensitive personal information.[111] The right to correct faulty

---

privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/AP2N-DEQE].

105. ANDREW B. SERWIN ET AL., PRIVACY, SECURITY, AND INFORMATION MANAGEMENT: AN OVERVIEW 35 (2011); 42 U.S.C. § 1320.

106. *See, e.g.,* CAL. CIV. CODE § 1798.120 (West 2022).

107. CAL. CIV. CODE § 1798.110 (West 2022).

108. *Id.*

109. *Id.*

110. CAL. CIV. CODE § 1798.105 (West 2022).

111. CAL. CIV. CODE §§ 1798.106, .121 (West 2022).

information allows consumers to request a business remedy inaccurate information obtained on the consumer.[112] Sensitive personal information is defined as personal information that includes "[a] consumer's precise geolocation, . . . genetic data, . . . racial or ethnic origin, religious or philosophical beliefs, . . . union membership, . . . social security, driver's license, state identification card, or passport number."[113] The definition encompasses any personal information involving someone's health, financial account information, sexual history, or sexual orientation.[114] A consumer may submit a request for a business to limit their use of the consumers' sensitive personal information to its proper service and function alone.[115] Essentially, the statute permits the business to use the information only for the reason the consumer initially provided it.[116] If the business wants to use the sensitive personal information in another manner, after receiving the initial request from the consumer, the business must receive informed consent for the additional use.[117] These supplementary protections guard consumers' most intimate information online; therefore, a Rhode Island data privacy statute should incorporate both of these rights.

A. *The Grave Harm to Consumers from Companies Sharing Their Sensitive Personal Information*

Consumers suffer a variety of harm from companies sharing consumers' sensitive personal information. The damage to consumers could be greater given the delicate nature of the information. For example, Grindr, a queer dating app, shared users' HIV status and GPS location with two companies that were examining the applications efficiency.[118] Sharing this type of intimate information

112. § 1798.106.
113. CAL. CIV. CODE § 1798.140 (West 2022).
114. *Id.*
115. § 1798.121.
116. *See id.;* Cheryl Saniuk-Heinig, *50 Years and Still Kicking: An Examination of FIPPS in Modern Regulation*, IAPP (May 25, 2021), https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation/ [https://perma.cc/MG3G-9Z7W] (This reflects the Fair Information Practice Principle (FIPP), "Use Limitation," which is mirrored in data privacy statutes around the globe).
117. § 1798.121.
118. Alison Bateman-House, *Why Grindr's Privacy Breach Matters to Everyone*, FORBES (Apr. 10, 2018), https://www.forbes.com/sites/

not only violates consumers privacy; but in some instances, it may threaten their physical safety.[119] Especially for individuals that are not "out," this information could be damaging to their livelihoods.[120] Moreover, the psychological effects from this type of breach could be far reaching.[121] A correlation was shown between a data breach and increased diagnoses of mental disorders resulting from the psychological trauma; others suffered psychological disturbances such as trouble sleeping, heightened stress levels, and psychosomatic symptoms.[122] This provides a stark illustration of the necessity of including additional protections for sensitive personal information within Rhode Island's data privacy statute. Furthermore, the provision should contain explicit safeguards for information related to an individual's sexual orientation and gender identity.[123]

B. *An Enforcement Mechanism to Empower Consumers*

A section of the CPRA provides for a civil cause of action in the event of a "Personal Information Security Breach."[124] If a consumer's personal information is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information," a consumer may bring suit.[125] The available remedies include injunctive or declaratory relief, monetary damages between $100-750 per consumer per incident, or actual damages.[126] A Rhode Island statute should include

---

alisonbatemanhouse/2018/04/10/why-grindrs-privacy-breach-matters-to-everyone/?sh=61ab7ceb67f4 [https://perma.cc/QZ5X-A9WM].

119. *See id.*

120. *See id.*

121. Ido Kilovaty, *Psychological Data Breach Harms*, 23 N.C.J.L. & TECH. 1, 18–19 (Sept. 2021).

122. *Id.* at 19.

123. CAL. CIV. CODE § 1798.140 (West 2022) (The current definition of sensitive personal information contained within the CPRA includes sexual orientation).

124. CAL. CIV. CODE § 1798.150 (West 2022).

125. *Id.*

126. *Id.* (The statute includes a non-exhaustive list of factors for determining damages: "the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the

a comparable private cause of action for consumers as a suitable enforcement mechanism.

V. THE POTENTIAL UNDESIRABILITY OF A COMPREHENSIVE DATA PRIVACY STATUTE IN RHODE ISLAND

Some opponents of a comprehensive data privacy bill in Rhode Island argue that a data privacy statute would be superfluous in the state. California is a massive technology hub, so passing a comprehensive bill makes sense in that region where it impacts major technology conglomerates.[127] Comparatively, Rhode Island is one of the smallest states in the United States, making it an inopportune place to enact a data privacy law with few big businesses operating in the state. Additionally, the rights contained in the CPRA should trickle down to other states because the technology conglomerates must abide by them for the massive populous residing in California.[128] Thus, it would be easier for companies to merely provide those rights to other states as well. For these reasons, opponents argue that implementing a comprehensive data privacy statute in Rhode Island would be redundant.

Unfortunately, California's enactment of the CPRA and the CCPA did not lead to an expansion of those rights to other states. The right to delete contained in the CPRA allows a consumer to require a business that gathered their personal information to erase it via a request form.[129] A unified system of submitting requests to businesses to erase consumer information is not available to residents in other states. The rights provided by the CPRA and CCPA are not often offered to people residing outside of California.[130] The internet, in many ways, serves as a great equalizer

misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth." The statute also provides open ended language for other plausible remedies.).

127. *See* Megan Graham, *California's New Privacy Law Puts Billions Worth of Personal Data under Protection*, CNBC (Jan. 3, 2020), https://www.cnbc.com/2020/01/03/californias-consumer-privacy-act-and-what-it-means-for-you.html [https://perma.cc/3Y5P-AWHK].

128. *See id.*

129. CAL. CIV. CODE § 1798.105 (West 2022).

130. *See* Graham, *supra* note 127 (Companies can elect to provide the rights contained in the CCPA and CPRA to consumers in other states. However, technology companies' business model and profit margins strongly rely on the

access to the internet provides the same capabilities and challenges whether you live in New York or Arkansas. However, with the passage of laws like the CPRA, consumers in California receive significantly more protection for their personal information online.[131] People residing in Rhode Island should be offered the same data privacy rights as people living in California.

A comprehensive data privacy law in Rhode Island could hurt businesses, particularly small businesses that gather some information on consumers, but its predominant business function and resulting profits do not involve data collection.[132] Creating the infrastructure to properly comply with the requirements set out in the CPRA could be costly for businesses.[133] For example, setting up a system to respond to requests to delete consumers' personal information could require hiring an additional employee which creates accompanying costs.[134] This concern is not unfounded, when the CCPA passed, compliance costs for California businesses for one year were approximated at fifty-five billion.[135] The CPRA creates financial barriers for small businesses and, thus, disincentivizes Rhode Island from passing a comprehensive data privacy statute.[136]

The CCPA includes a number of protections for small businesses which the CPRA expanded.[137] California intentionally targeted these statutes at influential technology conglomerates and carved out a number of exceptions for small businesses.[138] While some inevitable costs are associated with compliance, the CCPA only applied to companies that conduct business in California and

---

continuous source of consumers' personal data. Therefore, companies have no incentive to offer these data privacy protections).

131. *See* Alexandra Henry, *The California Consumer Privacy Act's Potential Incompatibility with the United States' Legal and Economic Landscape*, 23 SMU SCI. & TECH. L. REV. 227, 228 (2020) (listing four rights extended to California consumers).

132. *Id.* at 248–50.

133. *Id.*

134. *See id.* at 250.

135. *Id.* at 249.

136. *See id.* at 250.

137. Amrita Khalid, *Why Small Business Should Ignore California's Newest Data Privacy Law,* INC. (Nov. 10, 2020), https://www.inc.com/amrita-khalid/california-proposition-24-small-business.html [https://perma.cc/WQB7-ZCGB].

138. *See id.*

served "more than fifty thousand users, households, or devices;" the company's annual revenue exceeds twenty-five million; or half or more of their annual revenue is derived from selling consumers' personal information.[139] The CPRA further extended the protections for small businesses by providing that only businesses that serve more than one hundred thousand users or households annually must comply with the statute or satisfy the other threshold requirements.[140] This benchmark exists to protect small businesses from incurring disproportionate costs associated with complying with the statute while balancing the interest of providing vital privacy rights to consumers. Therefore, Rhode Island should adopt a similar safeguard for its small business owners to shield them from unsustainable compliance costs.

Since California passed the CCPA, Rhode Island has created multiple committees to research a suitable data privacy law for the state.[141] Thus far, Rhode Island has failed to enact a single data privacy statute to protect consumers' personal information. Perhaps, this lackluster response indicates an absence of political will and, consequently, shows consumer apathy about data privacy or a lack of cognizance about its importance. These additional protections contained in the CPRA are only effective if consumers take advantage of the rights provided. If Rhode Island adopted similar measures and consumers failed to exercise these rights, it would render the passage of a comprehensive, consumer-focused data privacy law futile.

There is an alternate explanation for the gridlock in the Rhode Island legislature regarding data privacy. While Rhode Island has not enacted any data privacy laws, a number have been introduced and the state has, to date, created two groups tasked with examining technological challenges: the Rhode Island Online Data Transparency and Privacy Protection House Commission (Commission) and the House Committee on Innovation, Internet, and Technology. The Commission is expected to release a report that contains legislative recommendations in the coming months.[142] Rhode Island

139. *Id.*; CAL. CIV. CODE § 1798.140 (West 2022).

140. Khalid, *supra* note 137; § 1798.140.

141. H.R. 8353, 2018 Jan. Sess. (R.I. 2018).

142. *Id.*; H.R. 6043, 2021 Jan. Sess. (R.I. 2021); The Commission was scheduled to release the report months ago which has not been released. Lynee Urbani, the Director of Policy for the RI Speaker of the House, said the

residents' indifference to data privacy is not an appropriate characterization; instead, Rhode Islanders need a combination of education to recognize the vulnerability of their data online and opportunity to exercise data privacy rights.

A meeting of the Commission provides an interesting illustration of interests present within these committees where no members of the general public were present.[143] However, the meeting was heavily attended by lobbyists, and "the commission itself is overstuffed with them."[144] The Commission is comprised of eleven members, five of whom are lobbyists for different interest groups: Michelle Cinquegrano, who represents Verizon; Christina Fisher, who represents Technet; Tom Wilkerson, who represents New England Cable and Telecommunications Association; Dr. Cedric Priebe, who represents Lifespan; and John Simmons, who represents Rhode Island Public Expenditure Council.[145] The remaining six members are Attorney General Peter Neronha and five members of the House of Representatives.[146] Some notable contributions from this meeting include Simmons' only addition, during which he expressed dismay about these policies damaging Rhode Island business competitiveness.[147] A lobbyist shared over the phone a similar concern about legislation involving data brokers being too severe.[148] Evidently, monied interests are overrepresented on the Commission and the interests of people residing in Rhode Island have fallen to the wayside.[149] Nonetheless, Rhode Island establishing these two committees shows the state's willingness to address data privacy challenges.

---

commission "very likely will meet again in 2022 in order to finalize findings and a report. There have been discussions at the hearings that have been held and we will be compiling the information for a report to be agreed upon by the commission after the new year."

143. Steve Ahlquist, *House Privacy Commission Overrun with Lobbyists*, UPRISE RI (Jan. 28, 2019), https://upriseri.com/2019-01-28-house-privacy/ [https://perma.cc/B2XN-SQQB].

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.*

148. *Id.*

149. *See generally id.*

A. *Rhode Island Legislative Recommendations*

Rhode Island's comprehensive data privacy statute should emulate California's newly-enacted scheme and include the right to delete, the right to correct inaccurate personal information, the right to know what personal information is being collected and the right to access personal information, the right to opt out of the sale of personal information, and the right to limit use and disclosure of sensitive personal information.[150] By including these pivotal provisions, consumers regain control and autonomy over their personal information. The statute should provide for a civil cause of action for consumers if a data breach occurs.[151] The civil action provides fundamental remedies for consumers after suffering considerable harm.[152] Minimally, a Rhode Island data privacy statute should incorporate these elements.

CONCLUSION

Consumers in Rhode Island are contained in a modern panopticon, an Orwellian nightmare, where companies watch their every move online, leaving consumers utterly powerless. Without decisive legislative action in Rhode Island, consumers will remain at the whims of technology giants to determine whether to grant consumers even a modicum of privacy. Rhode Island needs to pass a comprehensive bill to protect consumers' data privacy; the state took some action that indicates its amenability to protect consumers' personal information. A comprehensive data privacy statute in Rhode Island would correct this gross imbalance of power by affording consumers command over their own data.

150. CAL CIV. CODE §§ 1798.105–.106, .110, .120–.121 (West 2022).
151. CAL CIV. CODE § 1798.150 (West 2022).
152. *See id.*