June 11, 2024

Senate President Dominick J. Ruggerio
Senate Majority Leader Ryan W. Pearson
Senate Minority Leader Jessica de la Cruz
Speaker of the House K. Joseph Shekarchi
House Majority Leader Christopher R. Blazejewski
House Minority Leader Michael W. Chippendale
Rhode Island General Assembly
82 Smith Street
Providence, RI 02903

Re: Rhode Island HB 7787/SB 2500, Rhode Island Consumer Privacy Legislation — OPPOSE

Dear President Ruggerio, Majority Leader Pearson, Minority Leader de la Cruz, Speaker Shekarchi, Majority Leader Blazejewski, and Minority Leader Chippendale,

The undersigned organizations write in respectful opposition to HB 7787/SB 2500. The bill seeks to provide to Rhode Island consumers the right to know the information companies have collected about them, the right to access, correct, and delete that information, as well as the right to stop the disclosure of certain information to third parties. However, in its current form it would do little to protect Rhode Island consumers' personal information, or to rein in major tech companies like Google and Facebook. The bill needs to be substantially improved before it is enacted; otherwise, it would risk locking in industry-friendly provisions that avoid actual reform.

Consumers currently possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they collect and process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers' every move is constantly tracked and often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual orientation. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

At the same time, spending time online has become integral to modern life, with many individuals required to sign up for accounts with tech companies because of school, work, or simply out of a desire to connect with distant family and friends. Consumers are offered the illusory "choice" to consent to company data processing activities, but in reality this is an all or nothing decision; if you do not approve of any one of a company's practices, your only choices are to either forgo the service altogether or acquiesce completely.

We therefore offer several suggestions to strengthen the bill to provide the level of protection that Rhode Island consumers deserve:

- *Include strong data minimization rules to limit collection and use of personal data.* Privacy laws should set strong limits on the data that companies can collect and share so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out. We recommend including a strong data minimization requirement, like those recently passed as part of comprehensive legislation in Vermont and Maryland, that limits data collection to what is reasonably necessary to provide the service requested by the consumer, similar to the standard outlined in Consumer Reports' and EPIC's model bills.[1] In addition, a strong default prohibition on unnecessary data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for every business with which they interact.

- *Require companies to honor browser privacy signals as opt outs.* In the absence of strong data minimization requirements, at the very least, consumers need tools to ensure that they can better exercise their rights, such as a universal opt-out.. Unfortunately, it is not currently clear whether this bill supports the concept of universal opt-out signals, which would prevent consumers from being forced to contact hundreds, if not thousands, of different companies in order to fully protect their privacy.[2] This is not a theoretical problem; Consumer Reports recently conducted a study that found that, on average, more than 2,000 companies shared participants' consumer data with Facebook alone.[3] Making matters worse, Consumer Reports has documented that some companies' opt-out processes are so onerous

---

[1] *Model State Privacy Act*, Consumer Reports, (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/; *[STATE] DATA PRIVACY AND PROTECTION ACT*, EPIC, (February 22, 2023), https://epic.org/wp-content/uploads/2023/02/State-Privacy-Act-bill-text.pdf

[2] Section 6-48.1-5.(f) states that consumers can designate an authorized agent to effectuate their opt-out choices on their behalf, but is unclear what is encompassed by that term, especially when compared with other state privacy laws that clearly state that authorized agents include browser-level universal opt-out signals.

[3] Jon Keegan, Each Facebook User Is Monitored by Thousands of Companies, Consumer Reports, (January 17, 2024), https://www.consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companiesa5824207467/

that they have the effect of preventing consumers from stopping the sale of their information.[4]

The majority of comprehensive state privacy laws, such as those recently passed in Connecticut, New Hampshire, and Vermont, include such a provision. Privacy researchers, advocates, and publishers have already created a "Do Not Sell" specification, the Global Privacy Control (GPC), designed to work with the state privacy laws' global opt out provision.[5] This could help make the opt-out model more workable for consumers, but unless companies are required to comply, it is unlikely that consumers will benefit. We recommend using the following language:

> *Consumers or a consumer's authorized agent may exercise the rights set forth in this act by submitting a request, at any time, to a business specifying which rights the individual wishes to exercise. Consumers may exercise their rights via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt out.*

- *Apply privacy notice requirements to all controllers.* Section 6-48.1-3. creates privacy notice requirements that inappropriately only apply to "commercial websites" and "internet service providers." This Section should apply to any controller that is otherwise required to comply with the bill, as it is key to creating baseline transparency obligations that allow consumers to understand how their personal information is collected and used by the businesses with which they interact. This Section is also missing key requirements present in most other state privacy laws, including requirements for businesses to share information about how consumers can exercise their rights, provide links that allow consumers to opt-out, share information about the purposes for their collection or processing of personal data, and more.

- *Pseudonymous data exemption.* Section 6-48.1-7(m) of the bill seemingly stipulates that all consumer rights under the bill, including opt-outs, do not apply to so-called "pseudonymous" data. This represents a major loophole that would essentially exempt the majority of the online advertising ecosystem from the most substantive aspects of this bill's coverage. Online platforms and advertisers use pseudonymous identifiers (often mobile ad IDs or IP addresses) to track users across websites and apps, collecting extremely granular data about a user's search history, usage, personal characteristics, and interests in order to serve them targeted advertisements or to create a profile they can sell to other interested third-parties. Though this is precisely the type of online tracking this bill ostensibly seeks to grant consumers more control over, this exemption would allow vast swaths of it to continue

---

[4] Maureen Mahoney, Many Companies Are Not Taking the California Consumer Privacy Act Seriously, Medium (January 9, 2020), https://innovation.consumerreports.org/companies-are-not-taking-ccpa-seriously-the-attorney-general-needs-to-act/

[5] Global Privacy Control, https://globalprivacycontrol.org.

unabated. We presume that the intention of this provision is to minimize unnecessary data linkage as a result of a rights request. However, given the inclusion of the provision that restricts businesses from attempting to re-identify pseudonymous data in Section 6-48.1-7(k)(1), we question why the exemption is necessary at all.

- *Narrow the loyalty program exemption*. We are concerned that the exception to the anti-discrimination provisions in Sections 6-48.1-5.(b) and (c) when a consumer voluntarily participates in a "bona fide loyalty, rewards, premium features, discounts, or club card program" (Section 6-48.1-5.(d)) is too vague and could offer companies wide loopholes to deny or discourage consumer rights by simply labeling any data sale or targeted advertising practice as part of the "bona fide loyalty program." We urge the sponsors to adopt a more precise definition and provide clearer examples of prohibited discrimination that does not fall under this exception. For example, it's reasonable that consumers may be denied participation in a loyalty program if they have chosen to delete information or deny consent for processing that is functionally necessary to operate that loyalty program. That is, if you erase a record of having purchased nine cups of coffee from a vendor, you cannot expect to get the tenth cup for free. However, generally controllers do not need to sell data to others or to engage in cross-context behavior advertising in order to operate a bona fide loyalty program – such behaviors have nothing to do with the tracking of purchases to offer discounts or first-party advertising.

  Loyalty programs take advantage of the exact type of informational asymmetry that privacy laws should strive to eliminate. While consumers typically view loyalty programs as a way to save money or get rewards based on their repeated patronage of a business, they rarely understand the amount of data tracking that can occur through such programs.[6] For example, many grocery store loyalty programs collect information that extends far beyond mere purchasing habits, sometimes going as far as tracking consumer's precise movements within a physical store.[7] This information is used to create detailed user profiles and is regularly sold to other retailers, social media companies, and data brokers, among others. Data sales are extremely profitable for such entities — Kroger estimates that its "alternative profit" business streams, including data sales, could earn it $1 billion annually.[8] At a minimum, businesses should be required to give consumers control over how their information is collected and processed pursuant to loyalty programs, including the ability to participate in the program without allowing the business to sell their personal information to third-parties.[9]

---

[6] Joe Keegan, Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You, The Markup, (February 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you

[7] ibid.

[8] ibid.

[9] See Consumer Reports' model State Privacy Act, Section 125(a)(5) for an example of a concise, narrowly-scoped exemption for loyalty programs. https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/

- *Ensure targeted advertising is adequately covered.* We recommend refining the definition of "targeted advertising" to better match consumer expectations of the term. The drafted definition opens a loophole for data collected on a single site; it only includes ads based on a "consumer's activities over time and across nonaffiliated **websites**" (plural, emphasis ours). This would exempt "retargeted" ads from the scope of the bill's protections — ads based on one particular product you may have considered purchasing on another site. Such advertising — such as a pair of shoes that follows you all over the internet after you had left a merchant's site — are the stereotypical example of targeted advertising; the law's opt-out provisions should certainly apply to it. We suggest a shift toward the following definition:

  > *"Targeted advertising" means the targeting of advertisements to a consumer based on the consumer's activities with one or more businesses, distinctly-branded websites, applications or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. It does not include advertising: (a) Based on activities within a controller's own commonly-branded websites or online applications when the advertisement appears within that controller's own services; (b) based on the context of a consumer's current search query or visit to a website or online application; or (c) to a consumer in response to the consumer's request for information or feedback.*

- *Strengthen enforcement*. We recommend supplementing the bill's Attorney General enforcement with a private right of action, as was done in comprehensive privacy legislation recently approved by the Vermont legislature.[10] AG's offices typically have limited ability to enforce the law effectively against tech giants with billions of dollars a year in revenue. Consumers should be able to hold companies accountable in some way for violating their rights.

- *Remove entity level carveouts*. The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act, as well as covered entities and business associates under the Health Insurance Portability and Accountability Act. These carveouts arguably make it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire bill if one arm of their business receives enough financial information from banks or crosses the threshold into providing traditional healthcare services, a line many of them

[10] Though we'd recommend a further reaching private right of action, Vermont H. 121 at least provides for private enforcement that applies to large data holders and data brokers that violate the bill's provisions relating to sensitive data (see Section 2427(d)), https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0121/H-0121%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf

are already currently skirting.[11] At most, the bill should exempt *information* that is collected pursuant to those laws, applying its protections to all other personal data collected by such entities that is not currently protected.

- *Include strong civil rights protections.* A key harm observed in the digital marketplace today is the disparate impact that can occur through processing of personal data for the purpose of creating granularized profiles of individuals based off of data both collected and inferred about them. Therefore a crucial piece of strong privacy legislation is ensuring that a business' processing of personal data does not discriminate against or otherwise makes opportunity or public accommodation unavailable on the basis of protected classes. A number of privacy bills introduced in recent years have included such civil rights protections, including the bipartisan American Privacy Rights Act currently under consideration in Congress. Legislation approved in the Vermont and Maryland legislatures also include similar language.[12]

We look forward to working with you to ensure that Rhode Island consumers have the strongest possible privacy protections.

Sincerely,

Consumer Reports
Electronic Privacy Information Center (EPIC)
Restore the Fourth

cc: Sen. Louis Dipalma
Rep. Evan Shanley

[11] See e.g., The Economist, "Big Tech Pushes Further into Finance," (Dec. 15, 2022), https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance; Richard Waters, "Big Tech searches for a way back into healthcare," Financial Times, (May 17, 2020), https://www.ft.com/content/74be707e-6848-11ea-a6ac-9122541af204

[12] See, e.g., Vermont H. 121 Section 2419(b)(6)(A), https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0121/H-0121%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf