



epic.org

ELECTRONIC
PRIVACY
INFORMATION
CENTER



June 20, 2024

Governor Dan McKee
82 Smith Street
Providence, RI 02903

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

Dear Governor McKee,

The undersigned organizations write to urge you to veto HB 7787 Sub A as amended/SB 2500 Sub A as amended, legislation that was recently approved by the General Assembly. 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.

Big Tech has played a big role in the passage of weak state privacy bills. Of the 18 laws states have enacted so far, nearly all follow a model that was initially drafted by industry giants such as Amazon. HB 7787/SB 2500 follows that same model and is even weaker in many respects. If Rhode Island enacts this bill, you risk setting a new low bar for privacy protections in the United States.

While at a high level it may seem like HB 7787/SB 2500 is better than nothing, that is not the case. Rhode Islanders will be told they have "privacy rights," but due to the way the law is written, those rights are nearly impossible for the average Rhode Islander to exercise. Meanwhile, the Legislature will feel that they have already acted on consumer privacy and the chances of enacting a meaningful privacy law will decrease.

The key ways HB 7787/SB 2500 should be improved to provide meaningful protections for Rhode Island consumers include:

- *Implement 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 Maryland, which 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 use and 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 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 Maryland, include such a provision. Privacy researchers, advocates, and publishers have already created one such universal opt-out mechanism – a

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/>

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/>

“Do Not Sell” specification, the Global Privacy Control (GPC), designed to work with the state privacy laws’ global opt out provision.⁵

- *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 is out of step with other states, and 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.
- *Fix definitional inconsistencies.* The legislation currently uses the terms “personal data” and “personally identifiable information” interchangeably without defining the latter term. It is important that privacy legislation provides clear definitions for such key terms, so that consumers and businesses can understand which types of data are protected by the law. The current framework, for example, creates ambiguity as to when covered entities must provide privacy notices, which types of data sales need to be disclosed, and which statutory exclusions apply. Rhode Island would stand alone in creating this particular set of issues.
- *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. The Maryland Data Privacy Act, signed into law this year, also includes similar language.⁶

We raised additional issues with the bill in a letter to Senators before their vote. With all this in mind, we ask that you veto the legislation and urge the Legislature to strengthen the bill next session to provide the level of protection that Rhode Island consumers deserve.

⁵ Global Privacy Control, <https://globalprivacycontrol.org>.

⁶ 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>

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

Sincerely,

American Civil Liberties Union
American Civil Liberties Union of Rhode Island
Consumer Reports
Electronic Privacy Information Center (EPIC)
Restore the Fourth
U.S. Public Interest Research Group (PIRG)

cc: Sen. Louis DiPalma
Rep. Evan Shanley