March 13, 2025

Chair Wendy Harrison
Vice Chair Robert Plunkett
Senate Institutions Committee
Vermont Senate
115 State Street
Montpelier, VT 05633

Re: Vermont S. 71, Vermont Data Privacy and Online Surveillance Act — *SUPPORT*

Dear Chair Harrison and Vice Chair Plunkett,

Consumer Reports[1] strongly supports S. 71, which would create some of the most substantive state level privacy protections in the nation. The bill would require businesses to abide by strong data minimization provisions, which would prevent them from collecting or processing information that is not necessary to provide the specific product or service requested by consumers. It would also extend to Vermont consumers important new protections relating to their personal information, including prohibitions against selling sensitive data outright, a ban on the use of sensitive data for targeted advertisements, restrictions against targeting advertisements to children, and more.

Under current law, consumers 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, companies have amassed massive amounts of data about consumers, which is often combined with their offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is often retained for indeterminate amounts of time, sold as a matter of course, and is used to deliver targeted advertising, facilitate differential pricing, and enable opaque

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

algorithmic scoring—all of which, aside from reducing individual autonomy and dignity, can result in concrete harms for consumers, financial and otherwise.[2]

S. 71 corrects that imbalance by establishing strong privacy protections over consumers' personal information. In particular, we appreciate that S. 71 includes:

Strong Data Minimization Provisions

By far, S. 71's most important contribution to consumer privacy is Section 2419's prohibition against businesses collecting or processing personal information unless "reasonably necessary and proportionate" to provide or maintain "a specific product or service requested by the consumer to whom the data pertains." In today's digital economy, consumers are often faced with an all-or-nothing proposition: they may either "choose" to consent to a company's data processing activities, or forgo the service altogether if if they do not approve of any one of a company's practices disclosed in their privacy policy (which often allow the business to sell the consumer's information to vaguely defined third-parties).

S. 71 would turn this arrangement on its head by ensuring consumers' privacy by default and preventing individuals from having to take any action – either to opt-in or opt-out – to protect themselves. We know that measures based on an opt-out model (especially those without a universal opt-out provision) are destined to fail because they require consumers to contact hundreds, if not thousands, of different companies in order to fully protect their privacy. These opt-out processes are often so onerous that they have the effect of preventing consumers from stopping the sale of their information.[3] S. 71 instead puts the burden of privacy protection on those that otherwise have every incentive to exploit consumer data for their own benefit.

Sensitive Data Protections

Companies should not be profiting from the sale of consumers' most personal data, such as children's data or data about a consumer's race, religion, sex life, finances, precise geolocation, or health. The bill appropriately bans this behavior.

Some examples of harmful outcomes from the sale of consumers' sensitive data include:

---

[2] Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

[3] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Rights Protected, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-ConsumersDigital-Rights-Protected_092020_vf.pdf.

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use sensitive data to target vulnerable individuals for scams, or otherwise use personal information to cause harm. For example, scammers can use commercially available location data to increase the specificity of their phishing or social engineering scams, such as by including location-specific details, like mentioning a nearby business or the individual's recent activity.[4] Location data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.[5]

- *Predatory use of consumer data.* The sale of consumer data can result in financially disastrous consequences for consumers. Some data brokers sell lists of consumers sorted by characteristics like "Rural and Barely Making It" and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products. And a recent case brought by the Texas Attorney General alleged that the insurance company Allstate secretly purchased information about consumers' driving behaviors (including their precise geolocation data), which it used in some cases to raise consumers' premiums or deny them coverage altogether.[6] They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

- *Data breaches.* Data brokers sit on trillions of data points, many of them sensitive and purchased from other businesses. Unsurprisingly, this makes them a top target for hackers and cyber criminals. For example, the data broker Gravy Analytics, which has claimed to "collect, process and curate" more than 17 billion signals from people's smartphones every day,[7] reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.[8] This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[9]

---

[4] Phishing Box, Tracking Data: Identifying the Anonymized, https://www.phishingbox.com/news/post/tracking-data-identifying-anonymized

[5] Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs

[6] Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

[7] Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf

[8] Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/

[9] Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S.Military Personnel, (November 2023),

Strong Enforcement

Strong enforcement is key to ensuring that privacy laws provide more than theoretical protections for consumers. Unfortunately, most existing comprehensive privacy laws that only allow the Attorney General to bring cases aren't effective as they should be. There is ample evidence suggesting that there is widespread non-compliance with existing privacy laws. For example, two separate privacy compliance companies have found that the vast majority of top websites are not compliant with opt-out provisions under laws like CCPA.[10] Yet, there has not been commensurate enforcement efforts to remedy these issues to-date. In fact, to our knowledge, there are more states with active comprehensive privacy laws (13) than there have been total enforcement actions under those laws by Attorneys General.

S. 71 currently includes a limited private right of action that will allow consumers to hold certain companies liable for violations of certain provisions of the act. It allows for individuals to sue data brokers and large data holders (defined as companies that have collected 100,000 or more Vermont residents' personal data) when they have violated provisions of the law relating to sensitive data and consumer health data. This is a reasonable compromise that will ensure that the largest companies will be properly incentivized to comply with the law and that consumers can vindicate their rights relating to their most personal information, all while ensuring that Vermont's local businesses will still be able to compete while they get up to speed with the new law.

That said, while we think S. 71's allowance for both public and private enforcement mechanisms makes sense — dozens of other consumer protection laws do the same — and are generally skeptical of claims that such an approach would open the floodgates to frivolous litigation, we are open to discussing guardrails to prevent that outcome if raised in good-faith.

Protections for Data Collected Through Loyalty Programs

Section 2419(d)(2) of the bill currently includes common-sense protections that prevent controllers from ignoring consumers' privacy rights requests when they relate to data collected through loyalty programs. For example, the current language would prevent controllers from selling consumer data collected through loyalty programs for purposes unrelated to providing the benefits of the program.

---

https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf

[10] See, e.g. two separate studies indicating that less than 30 percent of top websites comply with universal opt-out requests: Privado, State of Website Privacy Report 2024, (December 2024), https://www.privado.ai/state-of-website-privacy-report-2024; Data Grail, Data Privacy Trends Report, https://www.datagrail.io/resources/interactive/data-privacy-trends/, (December 2024)

To be clear, we understand why privacy laws may need to include some exceptions to allow loyalty programs to function properly. 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, 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 the ability to offer first-party advertising.

This matches with consumer expectations around loyalty program data. In November 2024, Consumer Reports conducted a nationally representative survey of 2,108 adult American consumers and found that 70 percent of consumers who belong to loyalty programs would be at least somewhat concerned if a company sold information about them obtained through their loyalty program to other companies for unrelated purposes.[11] Moreover, 79 percent of Americans said they would support a law limiting companies to collecting only the data they need to provide customers with loyalty program benefits.[12]

While consumers typically view loyalty programs as a way to get rewards or save money based on their repeated patronage of a business, they typically do not expect all the secondary use and sharing of data that companies can engage in.[13] For example, many grocery store loyalty programs collect information that go far beyond mere purchasing habits, sometimes going as far as tracking consumer's precise movements within a physical store.[14] 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.[15] 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.

---

[11] Consumer Reports, November 2024 American Experiences Survey Omnibus Results, (November 2024), https://article.images.consumerreports.org/image/upload/v1734120809/prod/content/dam/surveys/Consumer_Reports_AES_November_2024.pdf
[12] *Id.*
[13] 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
[14] *Id.*
[15] *Id*.

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. We appreciate that S. 71 contains specific language prohibiting the use of personal information to discriminate against consumers.

******

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

Sincerely,

Matt Schwartz
Policy Analyst