S.71, An Act Relating to Consumer Data Privacy and Online Surveillance
House Commerce and Economic Development Committee
Megan Sullivan, Vice President, Vermont Chamber of Commerce
Joshua Diamond, Dinse, P.C., Special Counsel to the Vermont Chamber of Commerce.
April 30, 2026

The Vermont Chamber represents businesses of all sizes, in all industries, in every corner of Vermont. We understand what it takes to help businesses grow and thrive to build strong and vibrant communities, and our members have trusted us to center stewardship in our mission of advancing the Vermont economy. With this mission in mind we appreciate the opportunity to provide feedback S.71, An Act relating to Consumer Data Privacy and Online Surveillance.

We want to be clear at the outset: the Vermont Chamber supports comprehensive data privacy reform in Vermont.

Ideally, data privacy would be addressed at the federal level. Data and digital services do not operate within state boundaries, and a national framework would provide the consistency that both consumers and businesses need. However, in the continued absence of federal action, we recognize the responsibility states have taken on and support Vermont's work to move forward.

The Information Technology and Innovation Foundation[1] estimates that, without federal legislation, a patchwork of state laws could impose $20 to $23 billion in annual costs on U.S. small businesses. Related, the University of Vermont Legislative Research Service reported in 2025 that the average amount to implement California's new data privacy act was estimated to be $100,000 for medium sized businesses (20-100 employees).[2] Even assuming economies of scale that can be reached for Vermont, a portion of this amount will still create financial pressures for Vermont businesses. Economies of scale will be minimized if the law substantively departs from our regional neighbors. That is a scale of impact that warrants careful consideration as Vermont shapes its approach and why, since first engaging on data privacy legislation in 2023, we have consistently advocated for a framework that is compatible with laws adopted in other states.

Over the past year and a half, the Vermont Chamber has worked to deepen our technical knowledge of these issues by retaining Joshua Diamond of Dinse as special counsel. His strong background in consumer protection, including leading the creation of Vermont's data broker registry during his time in the Attorney General's office, brings valuable technical expertise to this discussion.

This engagement reflects a business community that is not seeking to avoid regulation but is committed to getting it right. Our goal is to support a framework that delivers meaningful protection for consumers while remaining workable for Vermont employers.

---

[1] The Looming Cost of a Patchwork of State Privacy Laws
[2] . Microsoft Word - Data Privacy Regulation.docx

Connecticut, New Hampshire, and Rhode Island have established a strong regional model for data privacy. S.71, as passed by the Senate, aligns with that framework. Today, we have submitted a letter signed by more than 100 Vermont businesses and organizations that reflects this position. It expresses strong support for comprehensive data privacy while urging Vermont to align with the regional framework reflected in S.71 as passed by the Senate. It also outlines concerns with provisions introduced in drafts since moving out of the Senate that are not compatible with approaches taken in neighboring states.

It is also important to address the timeline. S.71 was passed by the Senate more than 14 months ago. During that time Connecticut enacted additional updates to its data privacy law. While those updates have not yet been broadly adopted across the region, we welcome the opportunity to work with the committee to evaluate how those changes could be incorporated into Vermont's approach.

Any data privacy law will carry compliance costs. Those costs come at a time when Vermont businesses are already managing a long and growing list of cost and regulatory challenges. The question is not whether to act, but how to do so in a way that delivers strong consumer protections and allows Vermont businesses to succeed.

There is a path to achieve both. The current draft of S.71 does not yet strike that balance. Josh will walk through specific provisions and explain where the bill diverges from regional models and how those differences create challenges for Vermont's business community.

1. **Regional Consistency**.

Vermont businesses need legislation that aligns with our neighbors, specifically statutes that have been adopted on Connecticut, New Hampshire, and Rhode Island. This will provide a regional statutory scheme with shared definitions and applicability. Utilizing definitions and duties that align with other states provides meaningful protections for Vermont consumers, and it contains the continuity and consistency necessary for businesses to prosper and succeed in Vermont. This is accomplished in S.71 as passed by the Senate (S.71), which largely mirrors these statutes. In contrast, S. 71 version 2.3 (Version 2.3) contains unique definitions and operative terms, such as data minimization, that would leave Vermont on a regulatory island, which is bad for Vermont businesses and consumers.

As described below, Version 2.3's effect is overly broad, leaves Vermont with untested definitions, and sets up a game of gotcha that is inconsistent with creating a culture of compliance.

2. **The Applicability of Version 2.3 Is Overly Broad.**

Version 2.3 requires businesses that collect, use, store, analyze, delete, or modify any data that is linked to an individual consumer to provide complex and technical protections to consumers. Section 2415b(a)(1) provides that businesses who collect, use, store, analyze or modify data involving 35,000 consumers in a given year will need to comply with the technically demanding aspects of the legislation.
While this applicability standard is consistent with the regional laws in New England, Version 2.3 goes substantially further and captures many smaller businesses.

First, Version 2.3, § 2415b(a)(2) provides that anyone who controls or processes consumers' sensitive data, except for the purpose of completing a payment transaction, will be required to comply with the technically demanding aspects of the legislation. This will capture any business that collects, uses, or analyzes merely **one set** of sensitive data. Given the broad definition of sensitive data, as discussed below, this will likely capture any accounting practice, law firm, or other business that is helping a customer with their financial information or tax records. This one and done trigger for applicability.

Second, Version 2.3, § 2415b(a)(3) provides that anyone who sells personal data of consumers will be required to comply with the technically demanding aspects of the legislation. This is also a one and done trigger. Furthermore, the definition of sale is broad. It includes "the exchange of a consumer's personal data by the controller to a third party for monetary value or other *valuable consideration*." § 2415a(b)(52)(A). An illustration may help describe the broad sweep here. A candidate for public office maintains lists of likely voters who will support their candidacy. They share this information with their state or country party to assist with get out the vote activities. The candidate benefits from the get out the vote activities conducted by the party. This would likely satisfy the "valuable consideration" criteria, and now the candidate for office needs to fully comply with the comprehensive data privacy legislation.

The legislature should consider the size of the business or individual to be regulated. A one and done trigger is far too small to mandate the highly technical and expensive requirements of S. 71 or Version 2.3.

3. The Exemptions of S. 71 Are Too Narrow.

Version 2.3, § 2415c contains exemptions. Unlike bills in other states, there are no broad exclusions for non-profit entities, only those engaged in the government operation, certain entities regulated by the Vermont Department of Financial Regulation, victim services organizations, nonprofits that detect insurance fraud, and those involved in the news media and fraud detection. This leaves our non-profit sector, already under extreme pressure from the impending impoundment of federal dollars, subject to the obligations under this legislation.

In contrast, S.71 exempts non-profits that have c3 (charitable organizations), c4 (social welfare organizations), c6 (trade associations), and c12 (cooperatives) designations from the IRS. § 2415(24) and § 2417(a)(3).

4. Version 2.3 Utilizes Unique, Critical Definitions That Contain Ambiguities That Are Overly Broad or Too Narrow.

Version 2.3 either adds or significantly alters over 15 definitions contained in S. 71. Many of these are unique, without an analogue in other states. Here are several examples of concern for the The Vermont Chamber of Commerce:

- Publicly Available Information, Version 2.3 § 2415a(b)(48), contains an exception that is overly broad. There is general recognition that businesses should be able to access and utilize data that is not private and in the public realm without being subject to the restrictions of this legislation. However, the definition excludes public information that is "collated and combined to create a consumer profile that is made available…[on] a publicly available website…[or]…made available for sale." §§ 2415a(b)(48)(B)(ii) & (iii). This exception makes no logical sense to restrict the use of public information just because it was purchased from someone. Essentially, it would prohibit the use of data acquired from an old school "white pages" databases and subject the user to the duties and obligations of this very technical bill. It would likely include data acquired and processed by candidates for most county and statewide races here in Vermont. Such content based restrictions may also raise First Amendment concerns as well.[3]

  In contrast S.71's definition of public information is consistent with common, accepted understandings. It is information lawfully made available through federal, state, or municipal government records or widely distributed media, or that the consumer has lawfully made available to the general public. § 2415(33).

- Sensitive Data, Version 2.3 § 2415a(b)(53) contains a novel definition that is overly broad and vague. We agree there should be restrictions on the use of sensitive data. However, Version 2.3 uses an overly broad and novel definition. The novel definition includes "online activities of a consumer over time and across websites, online applications, online applications, and mobile applications, that do not share common branding, or data generated by profiling on such data." § 2415a(b)(53)(N).

  This definition is not limited to easily identified sensitive information such as biometric data, precise geolocation data, or consumer health data. It includes processing of any data from a first party owner that does not align with a common brand, much less affiliated entities. This significantly broadens what is subject to restrictions in the bill.

  Another example of the expanded and unique definition for sensitive data includes information that "reveals" a person's "philosophical beliefs." § 2415a(b)(83(B). Philosophical beliefs are not defined. In the absence of a clear definition, one might argue that philosophical beliefs could be deduced or revealed by voting in a particular primary election. If a candidate for office gathered such information to assist with get out the vote activities, they may become a "controller" for processing sensitive data and be subject to the regulatory requirements of Version 2.3.

  In contrast, S.71 uses a commonly recognized definition of data that reveals: (a) racial, ethnic, religious beliefs, mental health, sex life, sexual orientation,

[3]. *See Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011).

citizenship, and immigration status; (b) consumer health data; (c) genetic or biometric data for purpose of uniquely identifying an individual; (d) data collection from a known child; e) data concerning an individual's status as a crime victim; and (f) precise geolocation data. § 2415 (38).

Other notably unique definitions in Version 2.3, § 2415a(b) include:

- (12)(A), Context Advertising is … "advertisement that does not vary based on the identity of the individual recipient and solely based upon (i) immediate content of web page or online service within which the advertisement appears; (ii) specific request of the consumer for information or feedback. A controller may also use the "consumer's immediate presence within a geographic with a radius not than 10 miles or an area reasonably estimated to include online activity from at least 5000 users, but not including precise geolocation data." (12)(B)(ii).

  This definition will reoccur in the context of data minimization. It is noted that very few areas in Vermont likely satisfy "an area reasonably estimated to include on line activity from at least 5000 users."

- (23) First party advertising, …"processing by a first party of its own first party data for the purposes of advertising and marketing and is carried out: (A) through direct communications with the consumer such as email, mail, or text; (B) in a physical location operated by the first party; (C) through display or presentation of an advertisement on the first party's own website, application, or its online content.

  - First party is a consumer facing controller that the consumer intends to expects to interact. (22).

- (54)(A) Targeted Advertising, displaying or presenting an online advertisement…if
  - selected based, in whole or part, on known or predicted preferences, characteristics, behavior, or interests associated with the consumer or a device identified by a unique persistent identifier.
  - Includes… (an) advertisement based upon previous interaction of a consumer or a device identified by a unique identifier with such product or service on a website or online service that does not share common branding with the website or line line service…, and marketing measurement related to such advertisements.
  - It does not include first party advertising or contextual advertising.

5. Scope of Rights, Version 2.3, § 2415d.

S. 71 contains many of the same essential consumer protections in Version 2.3 and recognized by many states including: (1) confirmation that there is processing of personal data; (2) correct inaccuracies; (3) delete personal data; (4) obtain a copy of the personal data; and (5) opt out of targeted advertising or the sale of personal data or profiling in furtherance of decisions that produce legal or significant effects upon the consumer.

Version 2.3 adds a couple of additional consumer rights. A consumer has the right to obtain from the controller a list of the third parties to which such controller has sold the consumer's personal data or, if such controller does not maintain a list of the third parties to which such controller has sole the consumer's personal, a list of all third parties to which such controller has sold personal data… (a)(5).

It also includes the right to know whether a consumer's personal data were processed for the purposes of profiling in furtherance of any automated decision that produced any legal or similarly significant effect concerning the consumer, and if feasible: (i) question the results; (ii) be informed of the reason that such profiling resulted in such decision; (iii) review the data that was processed for such profiling; and (iv) and correct data if use is related to housing.(a)(7).

6. **Duty of Controllers, Version 2.3, § 2515e (Data Minimization).**

The duties for controllers in this section is called data minimization. However, Version 2.3 utilizes untested terms of art that differs from all other states. Its permitted uses of data are too narrow.

Version 2.3 provides that a controller shall limit the collection and processing of data to what is reasonably necessary and proportionate to provide or maintain:

- a specific product or service requested by the consumer to whom the data pertains. § 2515e(a)(1)(A);
- communication, other than an advertisement, provided it is reasonably anticipated within the context of the relationship with the consumer. § 2515e(a)(1)(B)
- may process or transfer the personal data of a consumer collected pursuant to subdivision (1) of this subsection to provide first party advertising or targeted advertising, unless (it is) (i) sensitive data; (ii) (the consumer opted out); or (iii) the controller know or willfully disregards that the consumer is a minor. § 2515e(a)(2).

- shall not collect or process sensitive data concerning a consumer except the processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains (a)(4).

- shall not sell sensitive data (a)(8)

Version 2.3 includes data minimization requirements that are confusing, overly restrictive, and it uses new language that is not used in any other jurisdiction. Version 2.3 significantly limits collection of data by a business to what is "reasonably necessary and proportionate…to maintain a specific product or service requested by the consumer to whom the data pertains; and a communication, that is not an advertisement, by the controller to the consumer that is reasonably anticipated within the context of the relationship between the controller and the consumer.

The language allows for limited targeted advertising from data collected pursuant to these limitations. However, the underlying limitations are significant and unprecedented. An illustration involving "retargeting" may be helpful. Retargeting occurs when a consumer visits a web site, and then the business sends the visitor an advertisement. This occurs when there is merely a specific visit to a web site. Retargeting occurs even when a consumer does not request a specific product or service. Version 2.3 would effectively prohibit this widely accepted form of targeted advertising.

Another example occurs when there are pooled advertising relationships. Version 2.3 would not allow a ski area to provide its contact list to ski clothing or ski equipment manufacturers who in turn want to provide discounted merchandise.

Version 2.3's limitations are too narrow. It unnecessarily inhibits the development of e-commerce by prohibiting businesses from processing data that does not fit closely within the box that requires a reasonably necessary and proportionate relationship with a specific product/service requested by the consumer. It also significantly limits consumer choice. Consumers may want opportunities to participate in cross marketing that Version 2.3 prohibits. A more reasonable approach that balances the needs of consumer and the creative economy is to allow collection and processing based upon notice. If sensitive data is involved, consumers must provide informed consent.

In contrast, S. 71 utilizes commonly accepted concepts of data minimization. They are tied to consumer disclosures, not guessing what is reasonably necessary and proportionate to the specific product or service requested by the consumer. A controller can collect and process data that is "adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer…" § 2420 (a). With proper conspicuous disclosure, this permits data to be utilized for targeted advertising. Some consumers appreciate this option. And, the consumer can always opt out. § 2518(a)(5).

7. Limits on The Processing of Sensitive Data, § 2419(c).

As previously noted in the definitions section, the universe of sensitive data under Version 2.3 is large. Version 2.3, §§ 2415e(a)(4) and (8) prohibit processing of sensitive data unless it is strictly necessary to provide a specific product or service requested by the consumer. The sale of sensitive data is absolutely prohibited.

The undefined term "strictly necessary" is overly broad. This would likely prohibit most basic data analytics by a company on different product lines or brands in its business.

Outright prohibition on the sale of sensitive data is also overly broad, especially since a sale includes any "valuable consideration." § 2415a(52)(A). The effects of these untested limitations would likely prohibit an affinity group from obtaining and utilizing data to invite like minded and interested folks to community gatherings, fundraisers, and offer specialized products and services sought after by members from the respective affinity group.

It may also prohibit a business that has multiple brands from analyzing and utilizing data for marketing from one entity to the other. See Version 2.3 § 2415a(b)(53)(N) that defines sensitive data as online consumer activities amongst websites that do not share common branding. For example an auto group with common ownership utilizes different branding between Subaru and Ford. The common owner or auto group would not be able to analyze and cross market.

A better way is notice and consent as set forth in Version 2.3. S. 71 allows for processing of sensitive data, and its potential sale, with affirmative, informed consent of the consumer. § 2420(a)(1).[4]

8. AGO Enforcement § 2424.

Verion 2.3 permits the AGO to enforce violations. However, there is no requirement for the AGO to offer a cure period during initial phases of implementation. Businesses should have an opportunity to cure, absent an AGO determination that a cure is not possible during the initial phases of implementing this very technical and complicated bill.

Furthermore, there is no safe harbor provision in the event a business comports with guidance issued by the AGO. S. 71 provides for both. See §§ 2425(b),(f).

9. S. 71 Provides Meaningful Protections to Consumers Against Data Security Threats.

S. 71 requires detailed security assessments. § 2422. In addition, controllers "shall establish, implement, and maintain reasonable, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue. § 2420(3)(e).

10. Conclusion.

---

[4]. Consent requires an affirmative act. Consent does not include acceptance of general or broad terms of use contained in a document with other unrelated information, hovering over, pausing, or closing a web page. § 2415(7).

S. 71 strikes the right balance of provides meaningful consumer protections, allowing businesses to operate in a modern economy that depends upon e-commerce, and provide regional consistency to assist in creating a culture of compliance.