S.71, An act relating to consumer data privacy and online surveillance
Senate Committee on Institutions

Megan Sullivan, Vice President, Vermont Chamber of Commerce
Joshua Diamond, Dinse, P.C., special counsel to the Vermont Chamber of Commerce.
March 11, 2024

The Vermont Chamber of Commerce 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.

The Vermont Chamber of Commerce supports comprehensive data privacy reform in Vermont. While data privacy ideally would be something handled at the federal level as data and digital services do not operate within the confines of the state's physical boundaries, we continue to see the federal government fail to act on this topic and we understand Vermont's need to set up and pride protections for consumers.

The Vermont Chamber of Commerce has had three consistent requests since first commenting on data privacy in 2023. First, Vermont's data privacy law needs to be regionally compatible. Second, the Attorney General needs to be the sole enforcement officer with the specific private right of action removed. Finally, there must be a robust education support for business to aid in compliance with this very complicated law.

These three requests reflect a business community that is not seeking self- regulation, but ready to participate in this process. However, policy proposals, such as those reflected in S. 71, move further away from being regionally compatible, with untested, ambiguous and confusing definitions, and the continued private right of action, we have serious concerns. We may be moving in a direction that results in businesses inadvertently failing to meet ambiguous standards that benefits class action lawyers rather than helping them achieve a culture of compliance that benefits consumers.

The Information Technology and Innovation Foundation (ITIF) has estimated that, in the absence of Congress passing federal privacy legislation, a patchwork approach of state privacy laws would have a substantial financial impact, with U.S. small businesses bearing a $20–23 billion dollar cost annually.
Connecticut, New Hampshire, and Rhode Island have created a regional model of data privacy, which bill S.93 is modeled after. Today, 18 business, non-profit, and medical organizations that are all based in Vermont, not the District of Columbia, sent out an op-ed expressing support for the approach S.93 takes to data privacy. See attached **Exhibit A**. I would ask you to keep in mind the responsible Vermont supported approach that S.93 offers.

Businesses and non-profits in Vermont are struggling. Three years of double-digit health care premium increases, property tax increases, a payroll tax, the economic uncertainly of tariffs and federal funding cuts. Any data privacy law will come with some level of compliance costs. There is a way to efficiently implement a comprehensive data privacy law that will streamline those costs while still offering comprehensive protection to consumers.

S. 71 does not meet the Vermont Chamber of Commerce's policy goals and concerns. It subjects Vermont businesses to highly technical and complex requirements that utilizes novel and untested concepts, instead of generally accepted language used throughout New England. In contrast, the Vermont Chamber of Commerce supports S. 93 as the preferred method to achieve meaningful consumer protections, create regional consistency for the business community to thrive, and focus enforcment within the authority of the Vermont Attorney General. Below is a list of the Vermont Chamber of Commerce's top concerns with S. 71.[1]

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 the Vermont consumer, and it contains the continuity and consistency necessary for businesses to prosper and succeed in Vermont. This is accomplished in S.93, which largely mirrors these statutes. In contrast, S. 71 would leave Vermont on a regulatory island, which is bad for Vermont businesses and consumers. As described below, its effect is overly broad, leaves Vermont with untested definitions, and sets up a game of gotcha with large class action law firms.

2. **The Applicability of S. 71 Is Overly Broad.**

S. 71 requires small 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 4 provides that by 2028, businesses who collect, use, store, analyze or modify data involving 6,250 consumers in a given year will need to comply with the technically demanding aspects of legislation.
Many Vermont businesses do not have in house IT professionals or specialized legal counsel to assist them with compliance. The applicability of S.71 would unnecessarily require compliance by many small businesses who are merely storing the data of their consumers or potential consumers.

[1] . The items identified in this memorandum are not intended to be comprehensive. They are an itemization of the Vermont Chamber of Commerce's top concerns.

Proponents of S. 71 have argued that application of the highly technical requirements of this legislation should be proportionate to the population of Vermont. This is an erroneous paradigm for application. The legislature should consider the size of the businesses to be regulated. Businesses that collect data on 6,250 Vermont consumers is far too small to mandate the highly technical and expensive requirements of S. 71.

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

§ 2417 contains exemptions. Unlike bills in other states, there are no broad exclusions for non-profit entities, only 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.93 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. **S. 71, § 2415 Utilizes Unique, Critical Definitions That Contain Ambiguities, Are Overly Broad or Too Narrow.**

The Vermont Chamber of Commerce is concerned about the following definitions:

- Consumer. This definition does not expressly exclude employees or those working in a commercial capacity like other states. Without this exclusion, this would create a whole new set of employee rights and limit reasonable management practices to ensure productivity in the workplace. Data collection related to productivity would be subject to an employee's right to demand access to the data, delete, and opt out. This could undermine reasonable productivity monitoring practices by an employer. § 2415(7).

  In contrast, S. 93 exempts employees and those working in a commercial capacity from the definition of consumer. § 2415(8)(B).

- First Party Advertising is too narrow, § 2415(22). Presumably, S.71 allows businesses to utilize consumer data it acquires from a visit by the consumer to its website, physical location, or online service for direct-to-consumer advertising.[2]

[2] . First party advertising is excluded from the definition of targeted advertising, which is subject to consumer opt outs. *See* §§ 2415(57)(B) and 2418(a)(7).

However, there is no recognition that to effectuate First Party Advertising most businesses need to transfer data to a third-party processor to effectuate the advertising. Failure to recognize this marketplace reality makes this concept unworkable.

S.93 does not utilize this concept because direct consumer advertising is permitted, including targeted advertisements from entities that are not from first parties. This process requires proper disclosure to consumers, who have the option to opt out. But, it effectively allows consumer choice for those who want the opportunity to access the benefits of targeted advertising from third parties.[3]

- Publicly Available Information, § 2415(50), 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." §§ 2415(50)(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.[4]

  In contrast S.93'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).

- Identified or Identifiable Individual, § 2415(32), contains technical, but undefined terms. This definition means "an individual who can be readily identified, directly or indirectly, including by reference to an identifier such as a name, an identification number, specific or historical pattern of geolocation data, or an online identifier." Precise geolocation data is defined in the bill. § 2415 (45), but there is no definition for specific geolocation data or a historical pattern of geolocation data. There is merit to protect the privacy expectations of precise

[3]. S.93, § 2420(a)(1) allows a controller to utilize personal that is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer. § 2418(a)((5)(A) allows for the opt out of targeting advertising.

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

geolocation data. However, this is just one example of using novel concepts without precise definitions that leaves businesses without practical guidance to ensure compliance with the law.

- Sensitive Data, § 2415(56) contains a novel definition that is overly broad and vague. We agree there should be restrictions on the use of sensitive data. However, S.71 uses an overly broad and novel definition. The novel definition includes "online activities of a consumer over time and across websites, online applications that do not share common branding, or data generated by profiling on such data." § 2415(56)(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 and opens up businesses to unnecessary litigation under the private right of action.

  In contrast, S.93 uses a commonly recognized definition of data that reveals: (a) racial, ethnic, religious beliefs, mental health, sex life, sexual orientation, 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).

5. Scope of Rights, § 2418.

Amongst the package of consumer rights contained in this section is the right to know whether personal data is or will be used in any artificial intelligence system and for what purpose. § 2118(a)(2). What is the difference between a software program that uses internal data with highly sophisticated algorithms versus another program that is considered "artificial intelligence." How will businesses know how to comply with this requirement in the absence of a definition?

S. 93 contains the basic consumer protections 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 without the novel, and undefined concepts found in S. 71.

6. Duty of Controllers, § 2519.

The duties for controllers in this section calls for data minimization. However, S. 71 utilizes untested terms of art that differs from other states. Its permitted uses of data are too narrow.

§ 2419(a) provides that collection is limited to that which is **reasonably necessary and proportionate.** Use of term "proportionate" injects a new term of art that is not utilized in other jurisdictions for the collection of data.

Collection and processing of must be tied to: (i) a specific product or service requested by consumer and (ii) communications, that are not an advertisement, by the controller to the consumer that is reasonably anticipated by the consumer within the context of the relationship between the controller and consumer.

This is too narrow, and it effectively prohibits targeted advertising, which is something some consumers want. It unnecessarily inhibits the development of the creative economy 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. 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. 93 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 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 S. 71 is large. § 2419(c) prohibits 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." § 2415(55)(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.

A better way is notice and consent as set forth in S. 93. S. 93 allows for processing of sensitive data, and its potential sale, with affirmative, informed consent of the consumer. § 2420(a)(1).[5]

8. AGO Enforcement § 2424.

S. 73 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. 93 provides for both. See §§ 2425(b),(f).

9. Private Right of Action § 2424(d).

S. 71 provides a private right of action to businesses that process data from 100,000 consumers, who earn gross revenues of $25 million, and involves violations of the obligations involving sensitive data. Given the broad definition of sensitive data, this could impact a number of VT businesses such as ski areas, larger grocery retailers, to nonprofits like hospitals.

Also, the available remedies include:

- $5000 or actual damages.
- Injunctive relief.
- Punitive damages for intentional violations.
- Reasonable attorneys' fees and costs.
- Any other relief that the court deems proper.

[5]. 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).

See § 2424(d)(2)(A).

Approximately 20 states have adopted comprehensive data privacy statutory schemes, but none of provided a private right of action. In each sister state, the Attorney General has exclusive enforcement authority. There is good reason for this trend. The private right of action will not create a culture of compliance; it will drive businesses away from Vermont with the threat of harassing lawsuits. Liquidated damages of $5000 along with the prospect to obtain additional punitive damages will likely inspire class actions, which do not get money to consumers, but pay plaintiffs' attorneys fees.

It is noted that punitive damages are not typically awarded in Vermont for mere intention violations, but those motivated by malice. The degree of culpability is much higher for malice that typically requires a showing of personal ill will.[6]

The AGO has the capacity to effectively enforce this law and create an effective deterrent to achieve compliance, especially given its current scope. This is not a unique when dealing with highly technical laws involving personal data. The AGO, along with DFR and the State's Attorneys, have exclusive authority to seek remedies for violations of the Security Breach Notice Act.[7]

In contrast, S. 93 does not have a PRA and expressly provides that the Attorney General shall have sole enforcement authority. § 2425(a).

[6] . *Kneebinding v. Howell*, 2018 VT 101, ¶ 87 ("Once a plaintiff establishes general damages…he may seek punitive damage if the defendant acted with malice…Malice may be shown by conduct manifesting personal ill will or carried out under circumstances evidencing insult or impression, or even by showing a reckless or wanton disregard for one's rights."

[7] . 9 V.S.A. § 2435(h) ("other than a person or entity licensed o registered with the Department of Financial Regulation…the Attorney General and State's Attorney shall sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter…").