S.71 Draft 4.2 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.
May 20, 2026

The Vermont Chamber of Commerce supports a comprehensive Data Privacy law that is regionally compatible. This serves several important policy objectives including: (1) protecting consumers; (2) helping ensure that Vermont businesses are not at a competitive disadvantage; (2) providing a common lexicon to help businesses interpret a complex regulatory scheme and achieve cultures of compliance.
The Vermont Chamber supports adoption of the regional model, including many of significant portions of the amendments passed by Connecticut in 2025 which will go into effect in July.
The draft as presented makes significant progress in aligning more closely with regional models, however, it contains definitions that result in significant departures from CT 2025 which concern the Vermont Chamber of Commerce's members. A list of concerns are as follows:

A. Definitions.

The Vermont Chamber of Commerce did not oppose the Kids Code legislation because it was narrowly tailored to address a vulnerable class, i.e., children, and did not broadly apply to the Vermont business community. Efforts to graft the kids code definitions into a statutory scheme that provides broad data privacy obligations do not fit.

Here are a few examples:

1. Biometric data. § 2415a(b)(3) While the list of attributes are okay, the introductory language contains ambiguities that are problematic. The definition starts with:

   "…means data generated from the technological processing of an individual's unique biological, physical or physiological characteristics that allow or confirm the unique identification of the consumer…."

   The "allow" language is inherently broad as opposed to "used to identify a specific individual," which is utilized in CT. "Allowing something to occur seems quite tangential as opposed to have a direct link such as "used."

2. "Personal data" §§ 2415(a)(37) and "deidentified data" references devices linked to a household.

   "…information, including derived data and unique identifiers, that is linked or reasonably linkable alone or in combination with other information…to a device that identifies, is

linked to, or is reasonably linkable to one or more identified or identifiable individuals in a household."

This is overly broad. First, there is no definition of a household. For example, could a household include a married couple who share a computer. The application of these circumstances could create unreasonable results or make it impossible for compliance. How would a controller know whether or not one spouse was entitled to opt out of targeted advertisements from the household computer when another spouse was okay receiving them on the same device. Even if there is a definition or other limiting principle of "household," it would be inherently inconsistent with the concept of an "individual" and the exercise of their individual rights under the data privacy act.

In contrast the definition as passed by the Senate, and utilized regionally, just states "…information that is linked or reasonably linkable to an identified or identifiable individual…"

The definition of de-identification also rests on this novel concept of "household." See § 2415a(18), and similar compliance concerns apply.

3. "Identified or identifiable" § 2415(a)(28) utilizes the concept of an "identification number." Use of such identification numbers is likely to be inherently necessary to effectuate the deidentification process. It seems like use of "identification number" in the definition creates an inherent inconsistency. The CT definition of "an individual who can be readily identified, directly or indirectly," seems to work in a cleaner generally accepted method.

4. Publicly available information. § 2415a(44). This definition and its exclusion are inherently problematic. As previously discussed in the Vermont Chamber of Commerce's testimony, the exception 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, or "an inference that is generated from [them]." 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, merely because it is subject to sale, may also raise First Amendment concerns.[1]

B. Applicability, § 2415b.

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

The chamber has concerns with the "one and done" provisions. We discussed some flexibility in two areas. First, the sale of sensitive data could have a lower threshold (less than 35,000) provided that the data minimization provisions allow the sale with expressed consent. However, the mere collection and processing should not be included.

In addition, the mere sale of data should not trigger applicability given the broad definition of sale to include "any other valuable consideration."

Such one and done provisions will unnecessarily burden the smallest of Vermont businesses and non profits.

C. Exemptions, § 2415c

The draft eliminates many entity level exemptions in the CT legislation. While these categories of businesses are not the Vermont Chamber of Commerce's primary membership, the failure to include non profits and institutions of higher learning are a significant departure from CT.

D. Data Minimization, 2415e.

The language does not follow CT (2025) regarding material changes in use of data. The Chamber is studying the language to fully understand the potential implications.

E. Enforcement. S. 71 as passed by the Senate contains an opportunity for a cure period during the initial phase of implementation (1.5 years). This provision should be reinstituted.