May 1, 2026

Rep. Michael Marcotte, Chair
House Committee on Commerce
and Economic Development
106 Private Pond Rd.
Newport, VT 05855

Rep. Edye Graning, Vice Chair
House Committee on Commerce
and Economic Development
115 State St.
Montpelier, VT 05633

Senator Alison Clarkson
18 Golf Avenue
Woodstock, VT 05091

RE: Letter in Opposition to Vermont S. 71

Dear Chair Marcotte, Vice Chair Graning, and Senator Clarkson:

On behalf of the advertising industry, we write to oppose Vermont S. 71.[1] We provide this letter to offer our non-exhaustive list of concerns about this bill. We support meaningful privacy protections for Vermont residents. As described in more detail below, S. 71 contains provisions that would make Vermont's privacy law significantly out-of-step with privacy laws in other states, thereby adding to the increasingly complex privacy landscape for both businesses and consumers across the country. Proposals such as these have been rejected in nearby New England states and Vermont should follow suit because of the deleterious effect these create for local economies.[2] Accordingly, we ask you to decline to advance the bill as drafted out of the Committee on Commerce and Economic Development ("Committee").

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,000 companies that power the commercial Internet, which accounted for nearly 20 percent of total U.S. gross domestic product ("GDP") in 2024.[3] By one estimate, approximately 18.2% of Vermont jobs in 2024 were related to the ad-subsidized Internet, a share projected to increase to 20% by 2029.[4] Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We would welcome the opportunity to engage with the Committee further on the points we discuss in this letter.

---

[1] Vermont S. 71 (2026 Session), located here, as amended by Draft. 2.3 here (hereinafter, "S. 71").
[2] *See* Maine Morning Star, *Fear of the unknown toll on businesses again likely to sink data privacy bill* (April 2026) located at https://mainemorningstar.com/2026/04/03/fear-of-the-unknown-toll-on-businesses-again-likely-to-sink-data-privacy-bill/.
[3] S&P Global, THE ECONOMIC IMPACT OF ADVERTISING ON THE US ECONOMY, 2024-2029 at 4 (Aug. 2025), located at https://theadcoalition.com/wp-content/uploads/2025/08/TAC_SP-Global-Final-Report_August-2025.pdf.
[4] *Id.* at 15-16.

I. Harmonization Across State Privacy Laws Fosters Consistency and Clarity for Consumers and Businesses

If enacted, S. 71 would make Vermont's approach to privacy an outlier in ways that would harm consumers and businesses of all sizes. Vermont should instead focus its efforts on harmonizing the bill with the approach to privacy in other states. A patchwork of differing privacy standards across the states would create significant costs for businesses and consumers alike. Efforts to harmonize state privacy legislation with existing privacy laws are critical to minimizing costs of compliance and fostering similar privacy rights for consumers no matter where they live. Below is a representative list of ways S. 71 would deviate from the consensus approach to privacy across states:

- S. 71's definition of "sensitive data" includes data no other state considers sensitive.
- S. 71 includes data minimization terms that are overly restrictive compared to other states.

Compliance costs associated with divergent privacy laws are significant. To make the point: a regulatory impact assessment of the California Consumer Privacy Act of 2018 concluded that the initial compliance costs to California firms would be $55 billion.[5] Another recent study found that a consumer data privacy proposal in a different state considering privacy legislation would have generated a direct initial compliance cost of $6.2 billion to $21 billion and ongoing annual compliance costs of $4.6 billion to $12.7 billion for the state.[6] Other studies confirm the staggering costs associated with varying state privacy standards. One report found that state privacy laws could impose out-of-state costs of between $98 billion and $112 billion annually, with costs exceeding $1 trillion dollars over a 10-year period, and with small businesses shouldering a significant portion of the compliance cost burden.[7] Harmonization with existing privacy laws is essential to create an environment where consumers in Vermont have privacy protections that are consistent with those in other states, while minimizing unnecessary compliance costs for businesses. Vermont should not add to this compliance bill for businesses and should instead opt for an approach to data privacy that is in harmony with already existing state privacy laws.

---

[5] *See* State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, 11 (Aug. 2019), located at https://dof.ca.gov/media/docs/forecasting/economics/major-regulations/major-regulations-table/CCPA_Regulations-SRIA-DOF.pdf.

[6] *See* Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida*, 2 (Oct. 2021), located at https://floridataxwatch.org/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=210&moduleid=34407&articleid=19090&documentid=986.

[7] Daniel Castro, Luke Dascoli, and Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Jan. 24, 2022), located at https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws (finding that small businesses would bear approximately $20-23 billion of the out-of-state cost burden associated with state privacy law compliance annually).

II. Online Activity Data Should Be Allowed for Use in Targeted Advertising and First-Party Advertising

S. 71 proposes a novel definition of "sensitive data" that includes online activity data, or information about an individual's online activities over time.[8] The bill would strictly prohibit using sensitive data, including online activity data, unless "strictly necessary" for providing or maintaining a consumer-requested product or service.[9] This approach, however, fails to recognize that online activity data is necessary for targeted advertising. Thus, while the bill would permit targeted advertising, it would ban the use of the very data that drives targeted advertising. By banning the use of online activity data for targeted advertising while simultaneously permitting targeted advertising subject to a consumer opt-out right, the bill proposes a confusing approach to targeted advertising that would have a chilling effect on commerce. No other state that has enacted an omnibus privacy law has taken this approach.

Online activity data should not be considered sensitive when used for an advertising purpose. Use of online activity data to deliver targeted advertising is permitted on an opt-out basis in every other state's privacy law. Furthermore, the use of data to deliver truthful, relevant advertising is protected by the First Amendment. The First Amendment protects both businesses in their right to free expression and individuals in their right to receive accurate information through advertising.[10] Vermont should not advance an approach to privacy that may run afoul of bedrock constitutional protections when other workable approaches to governing sensitive data processing are used across several states.

III. Overly Restrictive Limitations on Data Collection and Processing Would Stifle the Economy

S. 71 includes data minimization terms that would permit collection and processing of personal data only if reasonably necessary and proportionate "to provide or maintain… a specific product or service requested by the consumer to whom the data pertains."[11] This overly restrictive limitation on personal data processing would impede business' ability to process data for the benefit of consumers and to enrich the availability of goods and services in the economy. The proposed data minimization term could impose significant limitations on the availability of personal data for developing new technologies, providing pertinent messaging and advertising to consumers, creating cost-effective and efficient services, and combatting fraud.

For example, the term could functionally prohibit the collection of personal data to develop new and innovative offerings unrelated to requested products, or to improve existing offerings, because controllers would be prohibited from collecting data outside of the context of providing a specific product or service requested by the consumer. The term could also hinder

---

[8] *Id.* at § 2415a (b)(53)(N).
[9] *Id.* at § 2415e (a)(4).
[10] *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 756-67 (1976); *Sorrell et. Al. v. IMS Health Inc.*, 564 U.S. 552, 570-71 (2011).
[11] S. 71 at § 2415e (a).

businesses from cross-selling products and services to their own customer base because collection of data for such a purpose would not necessarily be tied to a product or service the customer already knew about or requested specifically. The term could also impede the general availability of personal data for prospecting, *i.e.*, taking steps to find new customers who may be interested in a business's products or services. In addition, the proposed term could severely inhibit third-party data sources from collecting personal data to further vital consumer fraud prevention and public safety efforts.[12] As a result of this data minimization term, third-party fraud prevention services may be forced to refrain from collecting and making data available that Vermont businesses rely on to prevent fraud, thereby making Vermonters more susceptible to identity theft and other negative outcomes.

The vast majority of states that have passed a data privacy law permit businesses to collect and process personal data as reasonably necessary and proportionate to achieve the purposes for which the personal data was collected, as disclosed to the consumer.[13] S. 71 would contradict this reasonable, majority approach, thereby subjecting Vermont consumers to fewer benefits of data processing than their counterparts in nearby states and other parts of the country. Vermont should take steps to align S. 71's data minimization terms with other states instead of adopting an onerous and untested approach to data collection and processing that could disadvantage Vermont consumers and businesses.

* * *

[12] *See* Digital Advertising Alliance, *Summit Snapshot: How Digital Ad Technology Helps Drive Amber System and Its Increasingly Global Impact* (Aug. 2024), located at https://digitaladvertisingalliance.org/blog/summit-snapshot-how-digital-ad-technology-helps-drive-amber-alert-system-and-its-increasingly.

[13] *See, e.g.,* Cal. Civ. Code § 1798.100(c); Va. Code Ann. § 59.1-578(1).

We and our members strongly support meaningful privacy protections for consumers. We believe, however, that S. 71 will not further meaningful consumer protection in Vermont and instead will diverge significantly from other state privacy laws, including the consumer privacy laws in Connecticut and New Hampshire. We therefore respectfully ask the Committee to decline to advance S. 71 as proposed.

Thank you in advance for your consideration of this letter.

Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
202-296-1883

Alison Pepper
EVP, Government Relations & Sustainability
American Association of Advertising Agencies, 4As
202-355-4564

Clark Rector
Executive VP–Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria
CEO
Digital Advertising Alliance
347-770-0322

CC: Members of the Vermont House Committee on Commerce and Economic Development

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP
Matthew Stern, Venable LLP