February 28, 2024

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

Representative Stephanie Jerome
Vice Chair of the House Committee on Commerce and Economic Development
PO Box 65
Brandon, VT 05733

Representative Logan Nicoll
Ranking Member of the House Committee on Commerce and Economic Development
11 Depot St.
Ludlow, VT 05149

RE: Ad Trade Letter in Opposition to Vermont H. 121, Draft 7.1

Dear Chair Marcotte, Vice Chair Jerome, and Ranking Member Nicoll:

On behalf of the advertising industry, we respectfully oppose Vermont H. 121, Draft 7.1 (hereinafter, "H. 121"),[1] and we offer this letter to express our non-exhaustive list of concerns about this legislation. We and the companies we represent, many of whom do substantial business in Vermont, strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, H. 121 would impose uneven requirements on different sectors of the digital economy and would create significant disharmony with current state-level privacy laws. H. 121 has unfortunately been amended to diverge even more substantially from existing state-level privacy laws. We provide these comments to illustrate how these divergent terms will, if enacted, hinder access to Internet-based resources in Vermont and impede the continued success of the state's small business community.

Vermont consumers deserve holistic privacy protections that are reasonably aligned with the privacy rights available to consumers in other states. By the same measure, Vermont businesses deserve assurances that they are not being disadvantaged as compared to enterprises in other states. We acknowledge that this is a complex task, and we encourage you to appropriately weigh these factors in striking a more reasonable balance which benefits consumers and the businesses which support so many Vermont jobs. We therefore encourage the House Committee on Commerce and Economic Development ("Committee") to update the bill to reflect the approach taken in the majority of other state privacy laws before advancing it through the legislative process.

[1] Vermont H. 121, Draft 7.1 (Gen. Sess. 2024), located here (hereinafter, "H. 121").

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country, including Vermont. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product ("GDP") in 2020.[2] 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.

I. Vermont Should Harmonize its Approach to Privacy with Other State Laws

We and our members support a national standard for data privacy at the federal level. In the absence of such a national standard, it is critical for state legislators to seriously consider the costs and confusion to both consumers and businesses that will accrue from a patchwork of differing privacy standards across the states. Harmonization with existing privacy laws is essential for creating an environment where consumers in Vermont have a consistent set of expectations and the same rights as individuals in other states, while minimizing compliance costs for businesses operating in Vermont. One way that H. 121 diverges from other states is by including in its definition of "consumer" any "individual who is in the State at the time a controller collects or processes the individual's data."[3] Other states cabin the definition of "consumer" to state residents.[4] H. 121's proposed definition would create additional compliance burdens for businesses—large and small—to understand where a given consumer is located when they process personal data associated with them. This construct could also have the unintended result of forcing companies to collect more information about individuals than they otherwise would have in order to comply with law. In addition, the bill's definition of "targeted advertising" does not match the definition set forth in other state laws.[5] This term should be updated to align with other states.[6]

Compliance costs associated with divergent—and oftentimes conflicting—privacy laws are significant. To make the point: one report found that differing privacy laws could impose costs of between $98 billion and $112 billion annually, with costs exceeding $1 trillion dollars over a 10-year period and small businesses shouldering a significant portion of the compliance cost burden.[7] We acknowledge that it is popular to think that these costs will impact only the biggest of companies, but in truth these costs (and any reduction in competition) will flow down to local

---

[2] John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located at https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf (hereinafter, "Deighton & Kornfeld 2021").

[3] H. 121 at § 2415(8)(a)(ii).

[4] *See, e.g.,* Cal. Civ. Code § 1798.140(i); Colo. Rev. Stat. § 6-1-1303(6); Conn. Gen. Stat. § 42-515(7).

[5] H. 121 at § 2430(45)(B)(iv).

[6] *See, e.g.,* Colo. Rev. Stat. § 6-1-1303(25); Conn. Gen. Stat. § 42-515(28).

[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).

retailers, travel destinations, recipe publishers, farm stands, restaurants, and myriad other small businesses who see digital advertising as the lifeblood of attracting customers. We encourage the Committee to take steps to align H. 121 with the majority of other state privacy laws that have been enacted.

II. H. 121's Requirement to Disclose Names of Specific Third-Party Partners Would Interfere with Legitimate Business and Create Competition Concerns

Another way H. 121 diverges from nearly all state privacy laws is that it would require controllers to disclose "a list of third parties, other than individuals, to which the controller has transferred … personal data" upon a consumer's request.[8] The vast majority of other states that have enacted privacy laws do not include this impractical and duplicative requirement. Instead, most other state privacy laws require companies to disclose the *categories* of third parties to whom they transfer personal data rather than the specific names of such third parties themselves.[9]

Requiring documentation or disclosure of the names of entities would be operationally burdensome, as controllers change business partners frequently, and companies regularly merge with others and change names. For instance, a controller may engage in a data exchange with a new business-customer on the same day it responds to a consumer disclosure request. This requirement would either force the controller to refrain from engaging in commerce with the new business-customer until its consumer disclosures are updated or risk violating the law. This is an unreasonable restraint.

From an operational standpoint, constantly updating a list of all third-party partners a controller works with would take significant resources and time away from their efforts to comply with other new privacy directives in H. 121. And the bill's amended language to give controllers an option to provide a list of names of third-party partners that receive data about a requesting consumer or a list of third-party recipients of any personal data does little to ease this operational burden.[10] Even with this option, controllers may be forced to jeopardize new business opportunities and relationships just to compile, maintain, update, and distribute these ephemeral lists.

International privacy standards like the European Union's General Data Protection Regulation ("GDPR") also do not require burdensome disclosures of specific third parties in response to data subject access requests, according to the text of the law. Mandating that companies disclose the names of their third-party partners could obligate companies to abridge confidentiality clauses they maintain in their contracts with partners and expose proprietary business information to their competitors. Finally, the consumer benefit that would accrue from their receipt of a list of third-party partners to whom a controller discloses data would be minimal at best. The benefit would be especially insignificant given H. 121 already requires controllers to disclose *categories* of

---

[8] H. 121 at § 2418(a)(2).
[9] *See, e.g.,* Cal. Civ. Code § 1798.110; Va. Code Ann. § 59.1-578(C); Colo. Rev. Stat. § 6-1-1308(1)(a); Conn. Gen. Stat. § 42-520(c)(5); Utah Rev. Stat § 16-61-302(1)(a).
[10] H. 121 at § 2418(a)(2).

third-party partners in privacy notices for consumers.[11] For these reasons, we encourage the Committee to reconsider this onerous language, which severely diverges from the approach to disclosures taken in almost all existing state privacy laws. To align H. 121 with other state privacy laws, the bill should require disclosure of the categories of third parties rather than the names of such third parties themselves.

III. H. 121's Data Broker Opt-Out Rights and Accessible Deletion Mechanism Provisions Would Create Unintended and Detrimental Results for Businesses and Consumers Alike

H. 121 would enact entirely novel data-broker-specific provisions. Such provisions are significantly unclear and would create confusion for both Vermont consumers and data brokers. Moreover, these provisions would unintentionally hinder consumers from accessing vital services that they rely on today. We ask the Committee to reconsider these ambiguous and unnecessary provisions and update them to be in line with the suggestions set forth in this letter.

As drafted, H. 121 would require data brokers to observe an "individual opt-out," permitting consumers to request that a data broker stop collecting data, delete all data in its possession about the consumer, and stop selling personal data about the consumer.[12] Data brokers would be required to honor such requests in 10 days, while all other controllers under the bill would be required to honor opt out requests within 45 days.[13] H. 121 would also require data brokers to observe a "general opt-out," permitting a consumer to request that all data brokers registered with the Secretary of State honor an opt-out request submitted via an online form to the Secretary of State.[14] The proposed opt-out rights are significantly unclear, as the bill provides little to no clarity regarding the differences between these opt-out rights or how they work together. Moreover, bill already permits consumers to opt out of sales, targeted advertising, and profiling by all controllers—including data brokers. The data-broker-specific opt-out rights are therefore duplicative of rights already contained in the bill; as currently drafted in H. 121, data brokers would just be required to effectuate opt-out rights at a much faster rate than other regulated controllers (10 days for data brokers as compared to 45 days for all other controllers). H. 121 would stand up these novel data broker choice structures—and their corresponding inequal timing requirements—without providing sufficient detail regarding how they will be managed. This constellation of rights will confuse and frustrate consumers and businesses alike.

H. 121 would also require the Vermont Secretary of State to maintain a "Data Broker Opt-Out List" denoting consumers who have opted out through the general opt out and require that list to "include an accessible *deletion* mechanism that supports the ability of an authorized agent to act on behalf of a consumer."[15] This provision conflates two different rights—opt out rights and deletion rights—with one another. The provision provides no clarity regarding how the "accessible

---

[11] *Id.* at § 2419(d)(1)(E).
[12] *Id.* at § 2448(a).
[13] *Compare id. with* § 2418(c)(1)(A).
[14] *Id.* at § 2448(b).
[15] *Id.* at § 2448(b)(8) (emphasis added).

deletion mechanism" would function in practice with the general opt-out required under the bill. Moreover, the provision introduces the possibility that authorized agents can submit these opt-out and/or deletion requests on behalf of consumers without any corresponding protection to ensure the agent is appropriately authorized by a consumer to act on their behalf.

Mass consumer opt outs—or deletion—of data from all data brokers through the click of a single button would stifle data brokers' ability to help power critically important products and services to Vermont citizens, such as anti-fraud and identity verification services, marketing services and loyalty programs, cybersecurity services, public interest research, risk management services, beneficiary location, and more. Even though H. 121 provides certain general exemptions, including an exemption for processing personal data to further security and integrity, such exemptions are structured to apply to controllers, processors, and consumer health data controllers.[16] The bill does not make clear that these exemptions similarly extend to data brokers. As a result, many beneficial consumer products—particularly those that further security and integrity efforts such as anti-fraud mechanisms—will be unavailable to consumers upon their use of the general opt-out or the accessible deletion mechanism set forth in H. 121. Many of these products depend on the transfer of personal data in order to authenticate consumer identities and root out fraud. This result is just one example of the many negative downstream impacts Vermont consumers will suffer if H. 121 is enacted as-is.

In addition, the proposed data-broker-specific opt-out and deletion rights would threaten the sustainability of the ad-supported Internet model, which subsidizes the largely free and low-cost availability of the online resources, products, and services that Vermont consumers enjoy today. According to one study, the free and low-cost products and services consumers access today—due in large part to data processed by data brokers—provides approximately $30,000 in value to each consumer every year, measured in 2017 dollars.[17] This significant cost-savings to Vermont residents would be eliminated if H. 121 is enacted as presently drafted. In addition, access to third party data via data brokers allows small and start-up businesses to reach audiences for their products and services in order to grow. The data-broker-specific opt-out and deletion rights in H. 121 would cut off a vital avenue for prospecting and consumer outreach that small businesses rely on to remain viable. H. 121's data-broker-specific rights should be harmonized with terms and opt-out rights in other states.

IV. H. 121's Private Right of Action Should Be Removed

As drafted, H. 121 would permit a private right of action for violations of its provisions.[18] We strongly believe private rights of action should have no place in privacy legislation. Instead, enforcement should be vested with the Vermont Attorney General ("AG") because such an enforcement structure would lead to strong outcomes for Vermont consumers while better enabling

[16] *Id.* at § 2426.
[17] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 21 (2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.
[18] H. 121 at § 2427(a)(2).

businesses to allocate resources to developing processes, procedures, and plans to facilitate compliance with new data privacy requirements. AG enforcement, instead of a private right of action, is in the best interests of consumers and businesses alike.

The private right of action in H. 121 will create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions will flood Vermont's courts with frivolous lawsuits driven by opportunistic trial lawyers searching for technical violations, rather than focusing on actual consumer harm. Private right of action provisions are completely divorced from any connection to actual consumer harm and provide consumers little by way of protection from detrimental data practices.

Additionally, a private right of action will have a chilling effect on the state's economy by creating the threat of steep penalties for companies that are good actors but inadvertently fail to conform to technical provisions of law. Private litigant enforcement provisions and related potential penalties for violations represent an overly punitive scheme that do not effectively address consumer privacy concerns or deter undesired business conduct. They expose businesses to extraordinary and potentially enterprise-threatening costs for technical violations of law rather than drive systemic and helpful changes to business practices. A private right of action will also encumber businesses' attempts to innovate by threatening companies with expensive litigation costs, especially if those companies are visionaries striving to develop transformative new technologies. The threat of an expensive lawsuit may force smaller companies to agree to settle claims against them, even if they are convinced they are without merit.

Beyond the staggering cost to Vermont businesses, the resulting snarl of litigation could create a chaotic and inconsistent enforcement framework with conflicting requirements based on differing court outcomes. Overall, a private right of action would serve as a windfall to the plaintiff's bar without focusing on the business practices that actually harm consumers. We therefore encourage legislators to remove the private right of action from the bill and replace it with a framework that makes enforcement responsibility the purview of the AG alone.

* * *

We welcome the opportunity to engage with you further about workable privacy standards to help ensure Vermont consumers maintain their access to and benefits from the information economy. **We ask the Committee to decline to move forward with H. 121 and to instead amend the bill to reflect the approach of the majority of states that have passed privacy laws.** As currently drafted, the bill sets forth a legal approach that would hinder Vermonters' ability to reap the benefits of a vibrant, ad-supported online ecosystem and Vermont businesses' ability to thrive.

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, 4A's
202-355-4564

Lartease Tiffith
Executive Vice President, Public Policy
Interactive Advertising Bureau
212-380-4700

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

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

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

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP