May 7, 2025

Senator Anne Carney
Chair of the Maine Judiciary Committee
3 State House Station
Augusta, Maine 04333

Representative Amy Kuhn
Chair of the Maine Judiciary Committee
2 State House Station
Augusta, Maine 04333

RE: Letter in Opposition to Maine LD 1822

Dear Chair Carney and Chair Kuhn:

On behalf of the advertising industry, we write to oppose Maine LD 1822.[1] We provide this letter to offer our non-exhaustive list of concerns about this bill. Our organizations support meaningful privacy protections for Maine residents. As described in more detail below, LD 1822 contains provisions that would make Maine's privacy law 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. Accordingly, we ask you to decline to advance the bill as drafted out of the Maine Judiciary Committee ("Committee").

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country that make up and support the digital economy. 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 and the digital economy, which accounted for 18 percent of total U.S. gross domestic product ("GDP") in 2024.[2] By one estimate, nearly 33,000 jobs in Maine are related to the ad-subsidized Internet.[3] We would welcome the opportunity to engage with the Committee further on the non-exhaustive list of issues with LD 1822 outlined here.

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

If enacted, LD 1822 would make the state's approach to privacy an outlier in ways that would harm consumers and businesses of all sizes. Maine 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 we provide a non-exhaustive list of ways LD 1822 would deviate from the dominant approach to privacy across states:

---

[1] Maine LD 1822 (132nd Maine Legislature), located here (hereinafter, "LD 1822").
[2] John Deighton and Leora Kornfeld, *Measuring the Digital Economy*, INTERACTIVE ADVERTISING BUREAU, 8 (April, 2025), located at https://www.iab.com/wp-content/uploads/2025/04/Measuring-the-Digital-Economy_April_29.pdf.
[3] *Id.* at 136 (estimating approximately 32,972 Internet-dependent jobs in the state of Maine).

- LD 1822 would include an overly restrictive limitation on personal data collection that would stifle the economy and impede the availability of data to improve products and services and combat fraud.
- LD 1822 would define "sensitive data" to include data elements no other state deems sensitive, would permit sensitive data processing only if "strictly necessary," and would flatly ban sales of such data, which would harm consumers' access to beneficial products and services.
- LD 1822 would require controllers to provide the names of their third-party business partners in responses to access requests, creating an onerous compliance requirement and competition concerns for controllers.
- LD 1822 would impose burdensome notice requirements on third parties that would not realistically account for ways in which these entities receive and process personal data.
- LD 1822 would include an untested "should have known" knowledge standard for determining minors' ages, creating confusion and adopting an approach to "knowledge" taken in no other state or federal privacy law.

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.[4] 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.[5] 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.[6] Harmonization with existing privacy laws is essential to create an environment where consumers in Maine have privacy protections that are consistent with those in other states, while minimizing unnecessary compliance costs for businesses. Maine 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.

II. Overly Restrictive Limitations on Data Collection Would Stifle the Economy

LD 1822 includes data minimization terms that would permit collection of personal data only if reasonably necessary and proportionate "to provide or maintain a product or service specifically

---

[4] *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/wp-content/uploads/sites/352/Forecasting/Economics/Documents/CCPA_Regulations-SRIA-DOF.pdf.

[5] *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.

[6] 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).

requested by the consumer to whom the data pertains."[7] This overly restrictive limitation on personal data collection 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 would 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 would also hinder 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 would severely inhibit third-party data sources from collecting personal data to further vital consumer fraud prevention efforts. 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 Maine businesses rely on to prevent fraud, thereby making Maine consumers 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.[8] LD 1822 would contradict this reasonable, majority approach, thereby subjecting Maine consumers to fewer benefits of data processing than their counterparts in nearby states and other parts of the country. Maine should take steps to align LD 1822's data minimization terms with other states instead of adopting an onerous and untested approach to data collection and processing that could disadvantage Maine consumers and businesses.

III. LD 1822's Restrictions on Sensitive Data Processing Would Hinder Delivery of Beneficial Services to Maine Consumers

LD 1822 would prohibit a controller from collecting, processing, or sharing sensitive data concerning a consumer, unless the collection or processing is "strictly necessary to provide or maintain a specific product or service requested by the consumer."[9] The bill would also flatly ban sales of sensitive data, without providing exceptions to this broad restriction for instances where consumers consent to sensitive data transfers or when such transfers are expected by consumers in the context of their relationship with controllers.[10] Given the bill's definition of sensitive data, which includes data elements that no other state considers sensitive (such as gender identity),[11] the proposed limitation on sensitive data processing and sales would severely hinder the delivery of beneficial products and services to Maine consumers. Instead of advancing this broad proposal, the Committee should amend

---

[7] LD 1822 at at Sec. 9608(2)(A).
[8] *See, e.g.,* Cal. Civ. Code § 1798.100(c); Va. Code Ann. § 59.1-578(1).
[9] LD 1822 at Sec. 9608(1)(A).
[10] *Id.* at Sec. 9608(1)(B).
[11] *Id.* at Sec. 9602(34).

the bill to mirror approximately 20 other state privacy laws that have been enacted to date by requiring consumer consent to process sensitive data.

Sensitive data is processed and transferred (i.e., "sold") to provide consumers with messaging about various products and services from which they derive significant benefits. Without the ability to "sell" and process sensitive data for advertising purposes subject to consumer consent, businesses will have a more difficult time, and face higher costs, reaching individuals with relevant marketing. For example, the provisions in LD 1822 could functionally prohibit religious organizations from reaching out to potential new parishioners and bespoke cultural product providers from reaching individuals of particular ethnicities with messaging and advertising about their products. The ability to use this data to advertise is also especially meaningful for Maine's small and medium-sized businesses who provide products and services that may be particularly relevant to specific constituencies.

The bill's ban on sensitive data sales and extreme limits on processing would also have other downstream effects. For instance, precise location data—a type of sensitive data under the bill—powers important emergency notices, particularly AMBER alerts and severe weather notices, allowing these notices to be immediately displayed to users in the impacted area on any device they are using. Location information also enables effective fraud prevention to protect consumers and businesses. Financial institutions, retailers, and others rely on anti-fraud services that include location information provided by third parties. The "sale" and processing of location information allows anti-fraud and identity protection services to flag suspicious behavior and protect vulnerable communities. For example, companies can more easily detect credit card theft or fraud if they or their service providers have access to location information showing that a consumer is not in the location where a purchase is being made. However, such processing may not be "strictly necessary" for providing a product or service requested by a consumer, and therefore, could be outlawed if LD 1822 becomes law. As a result, the Committee should update the bill to remove the onerous limits on sensitive data processing and the ban on sensitive data sales. The Committee should replace these provisions with a requirement for controllers to obtain consumer consent to process sensitive data.

IV. LD 1822 Would Diverge from Existing Privacy Laws by Requiring Controllers to Disclose the Names of Specific Third-Party Partners

Another way LD 1822 diverges from existing state privacy laws is that it would require controllers to disclose the names of their third-party partners in response to a consumer access request.[12] The overwhelming majority of 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 in response to access requests.[13] Requiring disclosure of the names of entities would provide little to no benefits to consumers, would not materially enhance consumers' understanding of controllers' data practices, and 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 access

---

[12] *Id.* at Sec. 9606(1)(F).

[13] *See, e.g.,* Cal. Civ. Code § 1798.110; Va. Code Ann. § 59.1-578(C); Colo. Rev. Stat. § 6-1-1301(1)(a); Utah Rev. Stat § 16-61-302(1)(a).

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 companies' efforts to comply with other new privacy directives in LD 1822.

Even international privacy standards like the European Union's General Data Protection Regulation ("GDPR") 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 where the cost clearly outweighs the benefit. For these reasons, we encourage you to reconsider this onerous requirement, which severely diverges from the approach to required disclosures taken in existing state privacy laws.

* * *

We and our members strongly support meaningful privacy protections for consumers. We believe, however, that LD 1822 will not further meaningful consumer protections in Maine and instead will diverge significantly from other state privacy laws in ways that will hinder Maine consumers' access to digital resources. We therefore respectfully ask the Committee to decline to advance LD 1822 as proposed.

Thank you 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

Michael Hahn
EVP & General Counsel
Interactive Advertising Bureau
212-380-4700

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

Lou Mastria
CEO
Digital Advertising Alliance
347-770-0322

CC: Maine Judiciary Committee

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

Chris Oswald
Advertising Trade Associations
LD 1822

Dear Chair Carney and Chair Kuhn:

Please find attached a letter from the following advertising trade associations in opposition to LD 1822: the Association of National Advertisers, the American Association of Advertising Agencies, the American Advertising Federation, the Interactive Advertising Bureau, and the Digital Advertising Alliance. We appreciate your consideration of this letter.

If you have any questions about this letter, please feel free to reach out to Chris Oswald at coswald@ana.net.

Best Regards,

Chris Oswald