February 23, 2022

The Honorable Senator Michael J. Rodrigues
Chair of the Massachusetts Senate Committee on Ways and Means
24 Beacon St., Room 212
Boston, MA 02133

The Honorable Senator Cindy F. Friedman
Vice Chair of the Massachusetts Senate Committee on Ways and Means
24 Beacon St., Room 313
Boston, MA 02133

RE: Letter in Opposition to S. 2687, the Massachusetts Information Privacy and Security Act

Dear Senator Rodrigues and Senator Friedman,

On behalf of the advertising industry, we oppose S. 2687, the Massachusetts Information Privacy and Security Act ("MIPSA").[1] We offer the following comments summarizing our primary, but non-exhaustive, list of concerns with the legislation as currently drafted, and we provide suggested amendments to the bill.

We and the companies we represent, many of whom do substantial business in Massachusetts, strongly believe consumers deserve meaningful privacy protections supported by reasonable government and responsible industry policies. However, state efforts to pass privacy laws only add to the increasingly complex privacy landscape for both consumers and businesses throughout the country. We and our members therefore support a national standard for data privacy at the federal level. If the Massachusetts legislature nonetheless decides to continue its effort to pass a privacy law in the state, we encourage it to consider an approach to privacy that aligns with recently enacted legislation in other states, such as the Virginia Consumer Data Protection Act ("VCDPA"). As presently drafted, MIPSA contains provisions that could hinder Massachusetts residents' access to valuable ad-supported online resources, impede their ability to exercise choice in the marketplace, and harm businesses of all sizes that support the economy.

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 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising expenditures. 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 you on our suggested amendments to MIPSA with an aim toward better aligning the wants of consumers with the needs of the Internet economy.

[1] S. 2687 (Mass. 2022), located here.

I. Massachusetts Should Take Steps to Harmonize Its Approach to Privacy With Other State Laws

Harmonization in state privacy law standards is in the interests of consumers and businesses alike, including those of Massachusetts residents. Uniformity helps to ensure consumers are subject to the same privacy protections no matter where they live and businesses can take a more holistic approach to privacy law compliance. MIPSA differs starkly from existing privacy laws, which would cause significant confusion for both businesses and consumers. Massachusetts should not adopt a law that differs from and competes with existing laws when alternative approaches exist that protect consumers while offering consistency across states. We encourage the legislature to examine already-enacted consumer protection standards that are available for regulating data privacy, including the VCDPA, before moving forward with MIPSA.

In the absence of a national standard for data privacy at the federal level, it is critical for legislators seriously to consider the costs 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 minimizing costs of compliance and fostering similar consumer privacy rights. 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.[2] Additionally, a recent study on a proposed privacy bill in a different state found that the proposal have generated a direct initial compliance cost of $6.2 billion to $21 billion and an ongoing annual compliance costs of $4.6 billion to $12.7 billion for the state.[3] 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 small businesses shouldering a significant portion of the compliance cost burden.[4] Massachusetts should not add to this compliance burden to businesses, and should instead opt for an approach to data privacy that is in harmony with already existing state privacy laws.

II. Broad Opt-in Consent Requirements Impede Consumers from Receiving Critical, Relevant Information and Messages

We urge legislators to take steps to clarify MIPSA's confusing provisions related to legal bases of processing and disclosures of sensitive information, and to work to align the bill's approach with existing state privacy laws. MIPSA offers Massachusetts residents the ability to limit the use and disclosure of sensitive information.[5] Additionally, the bill states that controllers must have a lawful basis to process sensitive information, but controllers cannot cite their own legitimate interests as such

---

[2] *See* State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 11 (Aug. 2019), located at https://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

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

[4] 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).

[5] MIPSA at Sec. 13.

a lawful basis for "selling" (*i.e.*, disclosing) sensitive information and must instead rely on consent or another lawful basis of processing to disclose such data.[6]

The bill consequently subjects sensitive information disclosures to a confusing dichotomy: on one hand, it provides consumers the ability to *opt out* of use and disclosures of sensitive information, and on the other hand, the bill appears to require *consent* or another lawful basis of processing that is not legitimate interests for a business to disclose sensitive information. We encourage the legislature to clarify this unclear approach to sensitive information by removing the lawful basis of processing requirements, which are present in no other state privacy law and set forth an ambiguous standard for permissible data processing activities. MIPSA should retain the consumer right to limit the use and disclosure of sensitive information, which is an approach that aligns with other existing state privacy laws.[7]

As discussed in more detail in Section V below, the data-driven and ad-supported online ecosystem benefits consumers and fuels economic growth and competition. Companies, nonprofits, and government agencies alike use data to send varying groups of individuals specific, relevant messages. Targeted messaging provides immense public benefit by reaching individual consumers with information that is relevant to them in the right time and place. Legal requirements that limit entities' ability to use demographic data responsibly to reach consumers with important and pertinent messaging, such as those set forth in MIPSA's sensitive information requirements, can have unintended consequences and, ultimately, serve as a detriment to consumers' health and welfare.

Ad-technology systems and processes enable everything from public health messaging to retailer messaging. They allow timely wildfire warnings to reach local communities and facilitate the dissemination of missing children alerts, among myriad other beneficial uses.[8] In accordance with responsible data use, uses of data for targeted advertising should be subject to notice requirements and effective user controls. Legal requirements should focus on prohibiting discriminatory uses of such data and other uses that could endanger the health or welfare of consumers instead of placing blanket opt-in consent requirements on uses of data.

One-size-fits-all opt-in requirements for data uses run the risk of regulating out of existence beneficial uses of information that help consumers, businesses, and non-profits by making messaging and information more relevant to individuals. Opt-in consent requirements also tend to work to the advantage of large, entrenched market players at the expense of smaller businesses and start-up companies. To ensure uses of demographic data to benefit Massachusetts residents can persist, and to help maintain a competitive business marketplace, we suggest that the Committee remove the bill's lawful basis of processing requirements for "sensitive information."

III. MIPSA's Proposed Global Opt Out Provisions Lack Reasonable Safeguards to Protect Consumer Choice

MIPSA would require the Massachusetts Attorney General ("AG") to conduct research on "the development of technology, such as a browser setting, browser extension, or global device setting, indicating an individual's affirmative, freely given, and unambiguous choice to opt out of the sale of the individual's personal information or limit the use or disclosure of the individual's personal

[6] *Id*. at Sec. 6(c).
[7] *See, e.g.,* California Privacy Rights Act of 2022, Cal. Civ. Code § 1798.121.
[8] *See* Digital Advertising Alliance, *Summit Snapshot: Data 4 Good – The Ad Council, Federation for Internet Alerts Deploy Data for Vital Public Safety Initiatives* (Sept. 1, 2021), located at https://digitaladvertisingalliance.org/blog/summit-snapshot-data-4-good-%E2%80%93-ad-council-federation-internet-alerts-deploy-data-vital-public.

information."[9] The provisions surrounding such required research should also instruct the AG to research and analyze necessary safeguards to: (1) ensure a preference indicated by a setting is a true expression of a consumer's choice, and (2) ensure certain businesses and models are not placed at an unfair disadvantage due to the implementation of such controls. Such safeguards are included in other state privacy laws, such as the California Privacy Rights Act of 2020 and the Colorado Privacy Act.[10] We urge you to amend MIPSA to include a directive to the AG to study such safeguards.

Choice settings must be designed and implemented in a manner that ensures a preference expressed through the setting is enabled by a consumer, and does not unfairly disadvantage or advantage one business or model over another. Otherwise, these settings run the risk of intermediary interference, as the companies that stand between businesses and consumers, such as browsers and others, can set such controls by default without requiring an affirmative consumer action to initiate the control. MIPSA should instruct the AG to research ways such safeguards can help avoid the unintended consequence of creating a new class of gatekeepers, which would undercut competition in the market. Unconfigurable, global opt out setting mechanisms have already been introduced in the market, making decisions for consumers by default without requiring them to affirmatively turn on the mechanisms.[11] These tools are not user-enabled, as they do not provide any assurance that consumers themselves are the ones making privacy choices. Consumers should be assured the ability to take an action to enable these settings, and such settings should be subject to specific parameters that ensure they do not unfairly advantage certain businesses at the expense of others. For these reasons, MIPSA should include a directive to the AG to study safeguards for such global controls that are included in other state privacy laws, such as safeguards to ensure global settings are not turned on by default and do not unfairly advantage one business or model over another.

IV. MIPSA Should Vest Enforcement Exclusively in the Massachusetts Attorney General

As presently drafted, MIPSA allows for private litigants to bring lawsuits if certain information associated with them is subject to a breach of security.[12] We strongly believe private rights of action should have no place in privacy legislation. Instead, enforcement should be vested with the Massachusetts Attorney General ("AG"), because such an enforcement structure would lead to strong outcomes for state residents while better enabling businesses to allocate funds 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.

A private right of action in MIPSA would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions would flood Massachusetts' 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, including a private right of action in MIPSA would have a chilling effect on the state's economy by creating the threat of steep penalties for companies that are good actors but

---

[9] MIPSA, Sec. 25(v)(1).
[10] California Privacy Rights Act of 2022, Cal. Civ. Code § 1798.185(a)(19)(A); Colorado Privacy Act, Colo. Rev. Stat § 6-1-1313(2).
[11] *See* Brave, *Global Privacy Control, a new Privacy Standard Proposal, now Available in Brave's Desktop and Android Testing Versions*, located here ("Importantly, Brave does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, the feature is on by default and unconfigurable.")
[12] MIPSA Sec. 7(e).

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 would not effectively address consumer privacy concerns or deter undesired business conduct. A private right of action would expose businesses to extraordinary and potentially enterprise-threatening costs for technical violations of law rather than drive systemic and helpful changes to business practices. It would 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 Massachusetts 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.

V. The Data-Driven and Ad-Supported Online Ecosystem Benefits Massachusetts Residents and Fuels Economic Growth

Over the past several decades, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A new study found that the Internet economy's contribution to the United States' gross domestic product ("GDP") grew 22 percent per year since 2016, in a national economy that grows between two to three percent per year.[13] In 2020 alone, it contributed $2.45 trillion to the U.S.'s $21.18 trillion GDP, which marks an eightfold growth from the Internet's contribution to GDP in 2008 of $300 billion.[14] Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet in 2020, 7 million more than four years ago.[15] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest internet companies, which generated 34 percent.[16] The same study found that the ad-supported Internet supported 217,220 full-time jobs across Massachusetts, more than double number of Internet-driven jobs from 2016.[17]

A. Advertising Fuels Economic Growth

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive legislation that significantly hinders certain advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy.[18] One recent study found that "[t]he U.S. open web's independent publishers and companies reliant on open web tech would lose between $32 and $39 billion in annual revenue by

---

[13] *See* John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 5 (Oct. 18, 2021), located https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf.
[14] *Id*.
[15] *Id*.
[16] *Id*. at 6.
[17] *Compare id.* at 127-28 (Oct. 18, 2021), located here *with* John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem,* INTERACTIVE ADVERTISING BUREAU, 106 (2017), located here (finding that Internet employment contributed 94,808 full-time jobs to the Massachusetts workforce in 2016 and 217,220 jobs in 2020).
[18] *See* John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located at https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf.

2025" if third-party tracking were to end "without mitigation."[19] That same study found that the lost revenue would become absorbed by "walled gardens," or entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.[20] Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated $15.5 billion in revenue.[21] Data-driven advertising has thus helped to stratify economic market power, ensuring that smaller online publishers can remain competitive with large global technology companies.

B. Advertising Supports Massachusetts Residents' Access to Online Services and Content

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content publishers offer consumers through the Internet, including public health announcements, news, and cutting-edge information about COVID-19. Advertising revenue is an important source of funds for digital publishers,[22] and decreased advertising spends directly translate into lost profits for those outlets. Since the coronavirus pandemic began, 62 percent of advertising sellers have seen advertising rates decline.[23] Publishers have been impacted 14 percent more by such reductions than others in the industry.[24] Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.[25] Legislative models that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, thereby compounding the detrimental impacts to the economy presented by COVID-19. The effects of such legislative models ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

C. Consumers Prefer Personalized Ads & Ad-Supported Digital Content and Media

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desire relevant ads, and a significant majority (86 percent) desire tailored discounts for online products and services.[26] Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers

---

[19] *Id*. at 34.
[20] *Id*. at 15-16.
[21] *Id*. at 28.
[22] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
[23] IAB, *Covid's Impact on Ad Pricing* (May 28, 2020), located at https://www.iab.com/wp-content/uploads/2020/05/IAB_Sell-Side_Ad_Revenue_2_CPMs_5.28.2020.pdf
[24] *Id*.
[25] *See* John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located at https://www.ipc.be/~/media/documents/public/markets/the-value-of-data-consequences-for-insight-innovation-and-efficiency-in-the-us-economy.pdf.
[26] Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located at https://www.thompsoncoburn.com/docs/default-source/Blog-documents/consumer-attitudes-toward-relevant-online-behavioral-advertising-crucial-evidence-in-the-data-privacy-debates.pdf?sfvrsn=86d44cea_0.

must pay for most content.[27] Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.[28]

During challenging societal and economic times such as those we are currently experiencing, laws that restrict access to information and economic growth can have lasting and damaging effects. The ability of consumers to provide, and companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the content we consume over the Internet is powered by open flows of information that are supported by advertising. We therefore respectfully ask you to carefully consider any future legislation's potential impact on advertising, the consumers who reap the benefits of such advertising, and the overall economy before advancing it through the legislative process.

* * *

We and our members support protecting consumer privacy. We believe MIPSA would impose new and particularly onerous requirements on entities doing business in the state and would unnecessarily impede Massachusetts residents from receiving helpful services and accessing useful information online. We therefore respectfully ask you to reconsider the bill and to amend the legislation.

Thank you in advance for consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Government Relations
Association of National Advertisers
202-269-2359

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Lartease Tiffith
Executive Vice President for 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: Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity

---

[27] Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.

[28] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.