COUNCIL for CITIZENS AGAINST GOVERNMENT WASTE

Thomas A. Schatz, *President*
1100 Connecticut Ave., N.W., Suite 650
Washington, D.C. 20036
ccagw.org

January 18, 2022

Alaska House Labor and Commerce Committee
Alaska State Capitol
120 4th Street
Juneau, AK 99801

Dear Representative,

On behalf of the 4,270 members and supporters of the Council for Citizens Against Government Waste (CCAGW) in Alaska, I urge you to vote against HB 159, which would impose restrictions and penalties on violations stemming from data brokering of consumer information.

Unfortunately, this bill will fail to achieve its objective to protect consumer privacy. Instead, it would create instability and uncertainty for companies doing business over the internet and their customers. The internet is not contained within a single state's boundaries and therefore participants operating within the internet ecosystem can only be regulated by the federal government under the Commerce Clause, Article I, Section 8 of the Constitution.

On December 14, 2017, the Federal Communications Commission adopted the Restoring Internet Freedom Order (RIFO), which restored the internet's proper classification as an information service, as intended in the 1996 Telecommunications Act. It was under this light-touch regulation that the internet thrived and became one of the greatest economic and social innovations in history.

The RIFO also reinstated the Federal Trade Commission's authority to investigate privacy and consumer protection violations by internet service providers (ISP) and strengthened its enforcement capabilities by enhancing transparency requirements. Any ISP infringing upon consumer privacy or engaging in otherwise unfair conduct can be held accountable for its actions.

States have enacted or will be reviewing laws that would protect personal information, including online privacy for children, websites, and monitoring employee e-mail communications. These laws would affect any business operating or selling to customers in each state, impinging on interstate commerce. Without the adoption of a consistent national privacy protection regime that preempts state and local laws, more states will enact their own rules, which raises costs and complicates compliance for businesses and individuals.

Rather than enact state laws imposing restrictions on online interstate commerce, the Alaska state legislature should encourage Congress to pass a national data privacy framework that will promote innovation while providing certainty across state borders for the regulation of data privacy.

Again, I urge you to vote against HB 159.

Sincerely,

Tom Schatz

January 25, 2022

The Honorable Rep. Zack Fields
Co-Chair of the House Labor and
Commerce Committee
State Capitol Room 24
Juneau, AK 99801

The Honorable Rep. Ivy Spohnholz
Co-Chair of the House Labor and
Commerce Committee
State Capitol Room 406
Juneau, AK 99801

RE: Letter in Opposition to Alaska HB 159 – Version I

Dear Representative Fields and Representative Spohnholz:

On behalf of the advertising industry, we oppose Alaska HB 159 – Version I ("HB 159").[1] We and the companies we represent, many of whom do substantial business in Alaska, strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, HB 159 contains provisions that could hinder Alaskans' 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.

To help ensure Alaskan businesses can continue to thrive and Alaskan consumers can continue to reap the benefits of a robust ad-supported online ecosystem and exercise choice in the marketplace, we recommend that the legislature undertake a study of available approaches to regulating data privacy before moving forward with enacting the onerous, and in some cases, outdated provisions set forth in HB 159. As presently written, the bill falls short of creating a regulatory system that will work well for Alaskan consumers or businesses. Below we address a non-exhaustive list of areas of concern with the bill at this time.

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 further study of the proposal with an aim toward better aligning the wants of consumers with the needs of the Internet economy.

I. Alaska Should Not Model Its Approach to Data Privacy Off of Outdated and Confusing Privacy Standards

Though HB 159 appears to draw many of its provisions from the California Consumer Privacy Act of 2018 ("CCPA"), the bill does not take into account many clarifications to the CCPA that followed its initial passage. The CCPA was amended more than five times after its enactment in June 2018, and the California Attorney General revised the regulations implementing the law four times after initially publishing draft regulations in October 2019. Many facets of the confusing and operationally complex law are still not fully tested or fleshed out. Moreover, the CCPA is not even the

[1] HB 159 – Version I (Alaska 2022) (hereinafter "HB 159"), located here.

most up-to-date privacy law in the state, as the California Privacy Rights Act of 2020 ("CPRA") was enacted, yet again materially amending California privacy law substantially. Further, the CPRA is a complex law that it not only relies on a yet-to-be-determined set of implementing regulations, but also a dedicated agency in California to continually interpret and update those initial regulations. Alaska should not adopt a legal regime that is outdated, confusing, or burdensome to Alaskan businesses and others operating in the state. Instead, we encourage the legislature to examine more current consumer protection standards that are available for regulating data privacy, including the Virginia Consumer Data Protection Act ("VCDPA"), before moving forward with HB 159.

As currently drafted, HB 159 also would create some of the most onerous requirements in the nation, potentially depriving Alaskans of valuable online content and services. For instance, the bill would require businesses to include a "Do Not Collect or Sell My Personal Information" link on their homepages that would appear to prohibit a covered business following an opt out from "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means, actively or passively receiving information from the consumer, or by observing the consumer's behavior."[2] Such a "do not collect" requirement, however, would prevent basic and vital Internet operations, including rendering a website to a visitor. This could result in many providers of online content and services to elect not to serve Alaskans, particularly given the threat of a private right of action which is included in the bill. Indeed, when the Federal Trade Commission recently opined on a related matter, it stated: "Privacy standards that give short shrift to the benefits of data-driven practices may negatively affect innovation and competition. Moreover, regulation can unreasonably impede market entry or expansion by existing companies; the benefits of privacy regulation should be weighed against these potential costs to competition."[3]

Efforts to emulate the CCPA in Alaska will significantly and disproportionately impact the ability of small and mid-size businesses and start-up companies to operate successfully in the state. A standardized regulatory impact assessment of the CCPA estimated *initial* compliance costs at 55 billion dollars.[4] This amount did not account for ongoing compliance expenses and needed resource allotments outside of the costs to businesses to bring themselves into initial compliance. Additionally, that same report estimated that businesses with less than 20 employees would need to spend $50,000 each to begin their CCPA compliance journey, and businesses with less than 50 employees would need to spend approximately $100,000 each.[5] Other studies confirm the staggering costs associated with varying state privacy standards. One report has 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.[6] Alaska should reconsider implementing outdated provisions of the CCPA, that now have been supplanted, as foundational aspects of its own privacy bill.

---

[2] HB 159, Sec. 45.49.940(7); Sec. 45.48.800(c)(1).

[3] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 11 (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.

[4] California Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act Regulations* at 11 (August 2019), located at https://www.tellusventure.com/downloads/privacy/calif_doj_regulatory_impact_assessment_ccpa_14aug2019.pdf.

[5] *Id*.

[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).

II. Proposed Global Privacy Control Provisions Lack Reasonable Safeguards to Protect Consumer Choice

HB 159 would require businesses to "treat the use of [a] global privacy control as a valid request submitted by the consumer" to opt out of sales, sharing, and disclosures of personal information and/or categories of personal information.[7] These provisions should be subject to further study by the Alaska legislature to ensure that any global privacy control requirement includes protections to guarantee that such controls are user-enabled, rather than turned on by default by technology intermediaries. HB 159's current provisions surrounding such controls are not accompanied by sufficient safeguards to ensure a preference indicated by a setting is a true expression of a consumer's choice.

Such controls 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.[8] 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. 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.[9] 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, the global privacy control provisions should be removed from HB 159.

III. HB 159 Should Not Include a Private Right of Action

As presently drafted, HB 159 allows for private litigants to bring lawsuits by deeming violations of the bill to be unfair or deceptive acts or practices under the Alaska Consumer Protection Act.[10] We strongly believe private rights of action should have no place in privacy legislation. Instead, enforcement should be vested with the Alaska Attorney General ("AG"), because such an enforcement structure would lead to strong outcomes for Alaskans 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 HB 159 would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions would flood Alaska'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.

---

[7] HB 159, Sec. 45.48.835(b).
[8] *See,* CPRA, § 1798.185(a)(19)(A); Colorado Privacy Act, § 6-1-1313(2).
[9] *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.")
[10] HB 159, Sec. 45.48.890; Alaska Stat. §§ 45.50.471 – 45.50.561.

Additionally, including a private right of action in HB 159 would 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 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 Alaska 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.

IV. The Data-Driven and Ad-Supported Online Ecosystem Benefits Alaskans 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.[11] 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.[12] 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.[13] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest internet companies, which generated 34 percent.[14] The same study found that the ad-supported Internet supported 11,855 full-time jobs across Alaska, almost double the growth in Internet-driven employment from 2016.[15]

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.[16] One recent study found that "[t]he U.S. open web's independent publishers and

---

[11] *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.

[12] *Id*.

[13] *Id*.

[14] *Id*. at 6.

[15] *Compare id.* at 121 (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 6,402 full-time jobs to the Alaska workforce in 2016 and 11,855 jobs in 2020).

[16] *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.

companies reliant on open web tech would lose between $32 and $39 billion in annual revenue by 2025" if third-party tracking were to end "without mitigation."[17] 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.[18] 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.[19] 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 Alaskans' 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,[20] 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.[21] Publishers have been impacted 14 percent more by such reductions than others in the industry.[22] Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.[23] 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.[24] 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 must pay for most content.[25] Indeed, as the Federal Trade Commission noted in its recent comments to

---

[17] *Id*. at 34.
[18] *Id*. at 15-16.
[19] *Id*. at 28.
[20] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
[21] 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
[22] *Id*.
[23] *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.
[24] 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.
[25] 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.

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.[26]

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 HB 159 would impose new and particularly onerous requirements on entities doing business in the state and would unnecessarily impede Alaska residents from receiving helpful services and accessing useful information online. We therefore respectfully ask you to reconsider the bill and instead convert it to a study so Alaskans can benefit from the legislature's careful consideration of approaches to data regulation that benefit consumers and businesses alike.

Thank you in advance for consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Head of 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: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

[26] 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.

February 7, 2022

The Honorable Rep. Matt Claman
Chair of the House Judiciary Committee
State Capitol Room 118
Juneau, AK 99801

The Honorable Rep. Liz Snyder
Vice Chair of the House Judiciary Committee
State Capitol Room 421
Juneau, AK 99801

RE: Letter in Opposition to Alaska HB 159 – Version I

Dear Representative Claman and Representative Snyder,

On behalf of the advertising industry, we oppose Alaska HB 159 – Version I ("HB 159").[1] We and the companies we represent, many of whom do substantial business in Alaska, strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, HB 159 contains provisions that could hinder Alaskans' 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.

To help ensure Alaskan businesses can continue to thrive and Alaskan consumers can continue to reap the benefits of a robust ad-supported online ecosystem and exercise choice in the marketplace, we recommend that the legislature undertake a study of available approaches to regulating data privacy before moving forward with enacting the onerous, and in some cases, outdated provisions set forth in HB 159. As presently written, the bill falls short of creating a regulatory system that will work well for Alaskan consumers or businesses. Below we address a non-exhaustive list of areas of concern with the bill at this time.

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 further study of the proposal with an aim toward better aligning the wants of consumers with the needs of the Internet economy.

I. Alaska Should Not Model Its Approach to Data Privacy Off of Outdated and Confusing Privacy Standards

Though HB 159 appears to draw many of its provisions from the California Consumer Privacy Act of 2018 ("CCPA"), the bill does not take into account many clarifications to the CCPA that followed its initial passage. The CCPA was amended more than five times after its enactment in June 2018, and the California Attorney General revised the regulations implementing the law four times after initially publishing draft regulations in October 2019. Many facets of the confusing and operationally complex law are still not fully tested or fleshed out. Moreover, the CCPA is not even the

[1] HB 159 – Version I (Alaska 2022) (hereinafter "HB 159"), located here.

most up-to-date privacy law in the state, as the California Privacy Rights Act of 2020 ("CPRA") was enacted, yet again materially amending California privacy law substantially. Further, the CPRA is a complex law that it not only relies on a yet-to-be-determined set of implementing regulations, but also a dedicated agency in California to continually interpret and update those initial regulations. Alaska should not adopt a legal regime that is outdated, confusing, or burdensome to Alaskan businesses and others operating in the state. Instead, we encourage the legislature to examine more current consumer protection standards that are available for regulating data privacy, including the Virginia Consumer Data Protection Act ("VCDPA"), before moving forward with HB 159.

As currently drafted, HB 159 also would create some of the most onerous requirements in the nation, potentially depriving Alaskans of valuable online content and services. For instance, the bill would require businesses to include a "Do Not Collect or Sell My Personal Information" link on their homepages that would appear to prohibit a covered business following an opt out from "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means, actively or passively receiving information from the consumer, or by observing the consumer's behavior."[2] Such a "do not collect" requirement, however, would prevent basic and vital Internet operations, including rendering a website to a visitor. This could result in many providers of online content and services to elect not to serve Alaskans, particularly given the threat of a private right of action which is included in the bill. Indeed, when the Federal Trade Commission recently opined on a related matter, it stated: "Privacy standards that give short shrift to the benefits of data-driven practices may negatively affect innovation and competition. Moreover, regulation can unreasonably impede market entry or expansion by existing companies; the benefits of privacy regulation should be weighed against these potential costs to competition."[3]

Efforts to emulate the CCPA in Alaska will significantly and disproportionately impact the ability of small and mid-size businesses and start-up companies to operate successfully in the state. A standardized regulatory impact assessment of the CCPA estimated *initial* compliance costs at 55 billion dollars.[4] This amount did not account for ongoing compliance expenses and needed resource allotments outside of the costs to businesses to bring themselves into initial compliance. Additionally, that same report estimated that businesses with less than 20 employees would need to spend $50,000 each to begin their CCPA compliance journey, and businesses with less than 50 employees would need to spend approximately $100,000 each.[5] Other studies confirm the staggering costs associated with varying state privacy standards. One report has 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.[6] Alaska should reconsider implementing outdated provisions of the CCPA, that now have been supplanted, as foundational aspects of its own privacy bill.

---

[2] HB 159, Sec. 45.49.940(7); Sec. 45.48.800(c)(1).

[3] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 11 (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.

[4] California Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act Regulations* at 11 (August 2019), located at https://www.tellusventure.com/downloads/privacy/calif_doj_regulatory_impact_assessment_ccpa_14aug2019.pdf.

[5] *Id*.

[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).

II. Proposed Global Privacy Control Provisions Lack Reasonable Safeguards to Protect Consumer Choice

HB 159 would require businesses to "treat the use of [a] global privacy control as a valid request submitted by the consumer" to opt out of sales, sharing, and disclosures of personal information and/or categories of personal information.[7] These provisions should be subject to further study by the Alaska legislature to ensure that any global privacy control requirement includes protections to guarantee that such controls are user-enabled, rather than turned on by default by technology intermediaries. HB 159's current provisions surrounding such controls are not accompanied by sufficient safeguards to ensure a preference indicated by a setting is a true expression of a consumer's choice.

Such controls 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.[8] 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. 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.[9] 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, the global privacy control provisions should be removed from HB 159.

III. HB 159 Should Not Include a Private Right of Action

As presently drafted, HB 159 allows for private litigants to bring lawsuits by deeming violations of the bill to be unfair or deceptive acts or practices under the Alaska Consumer Protection Act.[10] We strongly believe private rights of action should have no place in privacy legislation. Instead, enforcement should be vested with the Alaska Attorney General ("AG"), because such an enforcement structure would lead to strong outcomes for Alaskans 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 HB 159 would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions would flood Alaska'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, including a private right of action in HB 159 would have a chilling effect on the state's economy by creating the threat of steep penalties for companies that are good actors but

---

[7] HB 159, Sec. 45.48.835(b).
[8] *See,* CPRA, § 1798.185(a)(19)(A); Colorado Privacy Act, § 6-1-1313(2).
[9] *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.")
[10] HB 159, Sec. 45.48.890; Alaska Stat. §§ 45.50.471 – 45.50.561.

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 Alaska 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.

IV. The Data-Driven and Ad-Supported Online Ecosystem Benefits Alaskans 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.[11] 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.[12] 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.[13] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest internet companies, which generated 34 percent.[14] The same study found that the ad-supported Internet supported 11,855 full-time jobs across Alaska, almost double the growth in Internet-driven employment from 2016.[15]

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.[16] 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 2025" if third-party tracking were to end "without mitigation."[17] That same study found that the lost revenue would become absorbed by "walled gardens," or entrenched market players, thereby

---

[11] *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.

[12] *Id*.

[13] *Id*.

[14] *Id*. at 6.

[15] *Compare id.* at 121 (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 6,402 full-time jobs to the Alaska workforce in 2016 and 11,855 jobs in 2020).

[16] *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.

[17] *Id*. at 34.

consolidating power and revenue in a small group of powerful entities.[18] 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.[19] 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 Alaskans' 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,[20] 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.[21] Publishers have been impacted 14 percent more by such reductions than others in the industry.[22] Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.[23] 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.[24] 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 must pay for most content.[25] 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

---

[18] *Id*. at 15-16.
[19] *Id*. at 28.
[20] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
[21] 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
[22] *Id*.
[23] *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.
[24] 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.
[25] 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.

be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.[26]

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 HB 159 would impose new and particularly onerous requirements on entities doing business in the state and would unnecessarily impede Alaska residents from receiving helpful services and accessing useful information online. We therefore respectfully ask you to reconsider the bill and instead convert it to a study so Alaskans can benefit from the legislature's careful consideration of approaches to data regulation that benefit consumers and businesses alike.

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: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

[26] 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.

Computer & Communications Industry Association
Tech Advocacy Since 1972

February 8, 2022

Alaska House Judiciary Committee
Alaska State Capitol
120 4th St
Juneau, AK 99801

Re: CCIA Comments on HB 159, the Consumer Data Privacy Act

Dear Chair Claman, Vice Chair Snyder, and Members of the Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 159, the Consumer Data Privacy Act.

CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For fifty years, CCIA has promoted open markets, open systems, and open networks.[1] CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses (especially SMEs) have regulatory certainty in meeting their compliance obligations and that consumers are able to understand and exercise their rights.

While we appreciate the bill sponsor's efforts to protect the privacy rights of Alaskans and the tremendous work that has gone into drafting this legislation, we have concerns over the adoption of jurisdiction-specific legislation that would add to the existing patchwork of state privacy laws and respectfully ask that you oppose HB 159.

However, should the Committee proceed in considering the establishment of a new statewide consumer privacy framework, CCIA urges attention to the following principles in order to support meaningful privacy protections that avoid unnecessary interference with the ability of both consumers and businesses to benefit from data-enabled products, services, and innovations that support the modern economy.

1. **Clear and interoperable definitions**

Existing broad-based privacy laws typically recognize a core set of rights and protections including individual control, transparency of processing activities, and limitations on third-party disclosures that are reflected in HB 159. However, even minor statutory divergences between frameworks for key definitions or the scope of privacy obligations can create onerous costs for covered organizations. Therefore, CCIA encourages the legislature to ensure that any consumer privacy law enacted is reasonably aligned with definitions and rights in existing privacy

[1] For more information about CCIA please see: https://www.ccianet.org/about.

laws so as to avoid unnecessary costs to Alaska businesses, particularly as they focus on recovering from the fiscal impacts of the public health crisis.

As drafted, key definitions in HB 159 are likely to prompt significant statutory interpretation and compliance difficulties, even for businesses with existing familiarity with other US state laws. For example, both US and global privacy frameworks increasingly recognize the distinction between data "controllers" that determine how information is collected and used and data "processors" that perform operations on data on behalf of another entity, but this language is absent from HB 159. We encourage the Committee to consider the distinction between these differently situated entities and to ensure that any new privacy obligations are suited to the role that a covered organization plays with respect to personal data. CCIA further recommends attention to the recently enacted Virginia Consumer Data Protection Act and alignment of key definitions including "personal data," "sale," and "de-identified data" to promote consistent and practically operationalizable privacy protections across state borders.

2. **Vest enforcement authority with the Attorney General**

A new privacy framework would be best enforced by the office of the Alaska Attorney General. The inclusion of a private right of action could result in the proliferation of class action suits seeking lucrative settlements for alleged bare-procedural violations, primarily benefiting plaintiffs' attorneys with little connection to the remedy of any genuine consumer injury. The drawbacks of private rights of action are apparent in the history of both state and federal privacy statutes.[2] As drafted, the scope of HB 159's private right of action is far broader than any other US state commercial privacy law and threatens to uniquely burden Alaskan businesses without an obvious benefit to consumers' privacy interests.

3. **Mitigate operational burdens**

Implementing the requirements of a new privacy regime can be a lengthy and costly process for large and small businesses alike.[3] For example, covered organizations must review and potentially reconfigure IT systems and renegotiate contracts with vendors and service providers in order to comply with new rules. A successful privacy framework must ensure that businesses have sufficient opportunity and clarity to meet their compliance obligations. Recently enacted privacy laws in California, Colorado, Virginia, and Europe all contain 2-year delays in enforcement and we recommend that any privacy legislation advanced in Alaska include a comparable on-ramp to enable compliance.

---

[2] *See*, U.S. Chamber Institute for Legal Reform, "Ill-suited: Private Rights of Action and Privacy Claims" (July, 2019), https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf.

[3] For example, a study commissioned by the California Attorney General estimated that state companies faced $55 billion in initial compliance costs for meeting new privacy requirements, with small businesses facing disproportionately higher shares of costs. Berkeley Economic Advising and Research, LLC, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations'' (August, 2019), https://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

CCIA further supports the inclusion of an opportunity-to-cure provision in order to encourage organizations acting in good faith to rapidly resolve any concerns. This has been a successful enforcement mechanism in other jurisdictions and the California Attorney General recently highlighted the use of notices to cure as an effective tool in supporting widespread business compliance with new privacy rules.[4] Aligning this provision with the California Privacy Protection Act would provide more confidence for businesses operating in good faith to work with regulators in order to resolve any potential concerns.

** ** ** ** **

Thank you for your attention to the important subject of advancing consumer privacy protections and your consideration of these comments. CCIA respectfully asks that you oppose HB 159 at this time and stands ready to provide additional information and perspectives as the Committee considers consumer privacy issues.

Sincerely,

Alyssa Doom
State Policy Director
Computer & Communications Industry Association

[4] Xavier Becerra, "Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act" (March 15, 2021), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data.

Computer & Communications Industry Association
Tech Advocacy Since 1972

Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices

As the economy becomes increasingly data-focused, it is important for the U.S. to have a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights, transparent data processing, and organizational accountability. The digital economy is not constrained by state borders, and consumer interests and economic competitiveness will be best served by the development of baseline, federal privacy legislation. However, in the absence of a nation-wide framework, many lawmakers are debating whether to enact state-level consumer privacy rules. Though the adoption of divergent state privacy laws risks the emergence of a confusing and burdensome regulatory patchwork, carefully drafted state-level privacy legislation can also advance consumer protection while promoting the responsible processing of information that leads to data-enabled innovation and new technologies benefiting U.S. consumers and businesses. Therefore, CCIA presents these privacy principles to help inform stakeholders considering local privacy legislation.

Scope and Definitions

Effective consumer privacy legislation should clearly articulate what entities are subject to the law and to which types of data protections apply. Where practicable, policymakers should make an effort to align key definitions with consensus consumer privacy standards in both law and practice in order to promote regulatory interoperability and mitigate unnecessary compliance burdens.

- **Covered Organizations**: Legislation should extend to all private organizations that process personal information regardless of whether they have a direct or commercial relationship with an individual whose information they hold. Legislation should apply regardless of a business's sector or whether it collects information in an online or offline context. While some state privacy laws have excluded small businesses, policymakers should consider that potential risks resulting from the processing of personal data are not necessarily mitigated by the size of the data controller.

- **Personal Data**: Legislation should apply to information that is linked or reasonably linkable to a particular individual. While different types of personal data can vary in sensitivity depending on the context, some personal data is almost always sensitive and may warrant heightened protections under the law.[1] Furthermore, consumer privacy legislation should exclude publicly available information, as well as information that has been collected in an employment or business-to-business communications context, including as a job applicant

[1] U.S. state privacy laws have recognized certain discrete categories of "sensitive" personal data including: (1) information revealing racial or ethnic origin, religious beliefs, mental or physical health information, sexual orientation, and citizenship or immigration status; (2) biometric data processed for the purpose of uniquely identifying a natural person; and (3) data collected from a known child.

or as a beneficiary of someone acting in an employment context. Finally, in order to incentivize more protective data processing and storage, privacy laws should include carve-outs for information that is maintained in a de-identified or pseudonymous format.

- **Controllers and Processors:** Legislation should include a role-based distinction between "data controllers" that typically have a first-party relationship with data subjects and determine the collection and use of personal information and "data processors" that perform services on behalf of a controller. Data controllers are better situated to receive and implement the exercise of consumer rights while data processors should meet certain contractual obligations to support lawful and protective data use.

- **Exceptions:** Legislation should incorporate common sense exceptions to clarify requirements for covered organizations and to promote uniformity with international and domestic laws. Common exceptions include those for existing federal privacy regimes such as HIPAA, or exceptions for covered entities related to disclosure of trade secrets.

Consumer Rights

Consumers should feel confident they have control over their personal data, which will promote trust and participation in the digital economy. Privacy law should establish baseline rights for consumers over their personal information, no matter where it is collected or for what commercial purposes it is used.

- **Choice**: Legislation should empower consumers with greater choice over the use of their personal information. Leading jurisdictions have created **opt-out rights** for data processing for the purposes of sale to third parties, cross-platform targeted advertising, and profiling in furtherance of decisions with legal or similarly significant effects. For data processing that presents particular risks, policymakers should consider requirements that controllers obtain affirmative **consent** prior to the collection of sensitive data. Importantly, privacy law should align with the reasonable expectations of consumers, and avoid creating unnecessary friction that can result in "consent fatigue" or degrade user experiences.

- **Control**: Consumers should have the rights to reasonably **access**, **correct**, and **delete** personal information held by a covered organization. Furthermore, consumers should have the right to acquire data they have provided to a controller in a machine-readable, **portable** format when technically feasible. To protect against fraudulent requests, data controllers should be required to comply only with requests that are authenticated through commercially reasonable efforts. Controllers should not be empowered to require that consumers create new accounts to exercise requests, but should be able to require that consumers exercise requests via existing accounts.

- **No Retaliation:** Consumers should be protected from retribution from companies for exercising their privacy rights. However, this right should account for the fact that certain data processing is necessary for providing a requested product or service and include

exceptions for data processing that is relevant to participation in bona fide loyalty or other rewards programs.

- **Appeals:** Privacy legislation should require covered organizations to establish mechanisms for consumers to contest the denial of a consumer right under the law and to provide information for a consumer to contact the regulator to submit a complaint.

Responsibilities for Covered Organizations

In addition to empowering consumers with new rights, privacy legislation should require that covered organizations meet baseline standards for the safe and ethical use of personal data. Policymakers should consider the following threshold requirements applicable to organizations collecting, holding, and processing personal information.

- **Transparency:** Covered organizations should provide clear and accessible notices about the types of personal information that they are collecting and how they may use it. Effective notices should also state what categories of third parties personal information may be transferred to, and what choices and controls individuals have with respect to their personal information. Covered organizations should limit their collection of data to what is reasonably necessary for their clearly disclosed purposes.

- **Data Security:** Covered organizations should maintain a security program and follow reasonable measures to protect the confidentiality, integrity, and accessibility of personal information.

- **Risk Assessments:** Covered organizations that collect sensitive data or engage in processing that presents a heightened risk of harm to consumers should conduct and document a risk assessment that weighs the benefits and risks of data processing and applicable safeguards. Risk assessments should be producible to regulators conducting an investigation but should be otherwise exempt from public disclosure. Regulators should also accept risk assessments conducted pursuant to comparable legal regimes.

Ensure Practicable Compliance

The enactment of new consumer privacy legislation can be challenging and costly from a compliance perspective, and carries the risk of disproportionately impacting small and medium-sized organizations. To ensure that covered organizations have predictability in meeting their compliance obligations by the time a law becomes effective, privacy legislation should adhere to the following principles.

- **Technology Neutral:** Legislation should be principles-based, and afford differently situated organizations flexibility to meet legal standards by avoiding specific technological mandates.

- **Effective Date:** Complying with a new privacy law frequently requires covered organizations to engage in lengthy processes such as reviewing and potentially reconfiguring IT systems and renegotiating contracts with vendors and service providers. Legislation should allow covered organizations sufficient time for compliance, typically at least 18 months after a law's enactment.

- **Voluntary Consensus Standards**: Legislation should promote interoperable compliance across jurisdictions by recognizing and incentivizing participation in designated safe harbor programs and adherence to codes of conduct representing industry best practices for privacy and security.

- **Rulemaking:** Legislation should avoid sprawling rulemaking processes that could have the effect of turning a legal statute into a "moving target" and disincentivize early investment in compliance. Any rulemaking should be narrowly focused on specific implementation issues or enabling the law to be updated in light of changes in technology and business practices.

Enforcement

Privacy legislation should provide adequate funding for enforcement through the Attorney General or other comparable state consumer protection offices. Privacy laws should not include private rights of action, which have been shown to have the impact of attracting nuisance suits and distorting incentives away from risk-based compliance. Finally, in order to enable organizations acting in good faith to rapidly bring their data practices into compliance, legislation should include an **opportunity to cure** allegations of defective conduct prior to a formal enforcement action.

February 11, 2022

Dear Chair Claman, Vice Chair Snyder, and Members of the Committee,

Entertainment Software Association (ESA), the trade association representing video game publishers and console makers, respectfully submits this letter in opposition to Alaska House Bill 159. While ESA did not obtain the substitute bill prior to our oral testimony on February 7th, we remain interested in working with the committee on amendments that would align the bill with federal law on children's privacy and remove the private right of action.

During the House Judiciary hearing, members of the committee raised questions about the mechanics of obtaining parental consent. Although those questions were not directed to ESA, our industry has extensive experience complying with the well-established federal framework on children's privacy, which specifies procedures for obtaining parental consent and determining age.

An exemption providing data collected, maintained, and processed as required under the federal Children's Online Privacy Protection Act (COPPA) will align the bill with existing requirements for parental consent and avoid inconsistencies between federal and Alaskan law. The Federal Trade Commission (FTC) has given a lot of thought to parental consent and, under its rule implementing COPPA, identified a set of specific procedures that companies can rely upon to obtain parental consent for collecting personal information from minors under 13 years old. The currently approved procedures include:

- Signing a consent form and sending it back;
- Using payment authorization system that provides notice of each transaction to the account holder;
- Calling a toll-free number or video conference to interact with trained staff;
- Providing a copy of government-issued ID that can be checked against a database;
- Providing answers to a series of knowledge-based questions that would be difficult for someone other than the parent to answer;
- Verifying a picture of a photo ID to a second picture submitted by parent; and
- Sending an email to the parent and then having them respond with their consent. Then, the business sends a confirmation to the parent. This method, known as "email plus," may only be used where the information will be used for internal purposes and is not disclosed.

To adapt with evolving technology and consumer preferences, this list has evolved over time. In fact, the FTC is currently reviewing its COPPA Rule (Rule) and considering further updates to its list of approved methods as part of its COPPA Rule review process that began in 2019. Further, the Virginia Consumer Data Protection Act incorporates an exemption for parental consents obtained as required under COPPA, and the Colorado Privacy Act incorporates an exemption for all data collected in compliance with COPPA.

House Bill 159 is also not aligned with the federal standard for determining when a business is accountable to know the age of the user. The FTC has long held that a bright line approach to determining age, which sets forth a clear standard, is needed. For this reason, under both the COPPA statute and Rule, the legal standard is "actual knowledge" that the user is under 13 years old. The constructive knowledge standard, triggered by the "recklessly disregards" language proposed in HB 159, may be impossible to operationalize and leaves too much ambiguity as to when a business would run afoul of the bill.

Moreover, to minimize risk of noncompliance, a business would seem to be required to collect the age of every individual from whom it collects information to avoid violating the constructive knowledge standard. As a practical matter, this proposal would invite *more* data collection from businesses seeking to adhere to the rule, which should not be the result of any privacy legislation. The FTC has consistently rejected proposals to modify the COPPA Rule's actual knowledge standard for this reason, among others.

This ambiguity on age determination, when coupled with the bill's private right of action, creates an environment ripe for exploitation by plaintiffs' lawyers. ESA opposes the inclusion of a private right of action within the bill.

Consumer technologies are ever evolving, and accordingly, so too are the regulatory frameworks used to empower consumer transparency and choice. We encourage lawmakers to leverage the work done at both the federal and state level and clarify that parental consent obtained consistent with COPPA's requirements satisfies parental consent requirements under HB 159 for consumers who are under 13 years old. The committee members' questions raised during the House Judiciary hearing signal the committee's thoughtful approach to privacy, and ESA looks forward to future collaboration to develop a workable solution on this issue.

Sincerely,

Michael Warnecke
Chief Counsel, Technology Policy
Entertainment Software Association

February 11, 2022

The Honorable Matt Claman
State Capitol Room 118
Juneau, Alaska 99801

RE: House Bill 159 – Consumer Personal Information Privacy Act

Dear Representative Claman,

Thank you for your service and effort to protect consumer data with House Bill 159, the Consumer Personal Information Privacy Act. We support protecting consumer data and privacy. However, we encourage the Alaska Legislature not to pass a unique consumer and data privacy law, but rather encourage Congress to pass a national data privacy framework.

While we wholeheartedly support consumer data privacy and follow many stringent and best-practice consumer privacy policies at Alaska Communications, we also believe these frameworks should be developed and adopted at a national level rather than at the state level.

A state-by-state consumer data and privacy approach would create different regulations in different states, making it cumbersome and complicated for businesses to follow.

Rather than enact state laws imposing restrictions on online interstate commerce, the Alaska state legislature should encourage Congress to pass a national data privacy framework that will promote innovation while providing certainty across state borders for the regulation of data privacy.

Thank you for considering Alaska Communications perspective on this legislation. Please let us know if we can provide further information.

Sincerely,

Heather Cavanaugh
Director, External Affairs and Corporate Communication

COUNCIL for CITIZENS AGAINST GOVERNMENT WASTE

Thomas A. Schatz, *President*
1100 Connecticut Ave., N.W., Suite 650
Washington, D.C. 20036
ccagw.org

March 17, 2022

Alaska House Judiciary Committee
Alaska State Capitol
120 4th Street
Juneau, AK 99801

Dear Representative,

On behalf of the 4,271 members and supporters of the Council for Citizens Against Government Waste (CCAGW) in Alaska, I urge you to vote against HB 159, which would impose restrictions and penalties on violations stemming from data brokering of consumer information.

While we understand the desire to attempt to tamp down on violations incurred during data brokering of consumer information, this bill will unfortunately fail to achieve that objective. Instead, it would create instability and uncertainty for companies doing business over the internet and their customers. The internet is not contained within a single state's boundaries and therefore participants operating within the internet ecosystem can only be regulated by the federal government under the Commerce Clause, Article I, Section 8 of the Constitution.

Because of inaction by Congress, several states have enacted or will be reviewing laws to protect personal information, including online privacy for children, websites, and monitoring employee e-mail communications. These laws would affect any business operating or selling to customers regardless of the state in which either the business or customer are located, impinging on interstate commerce. Without the adoption of a national privacy protection framework that preempts state and local laws, more states will continue to enact their own separate rules, raising costs and complicating compliance for businesses and individuals.

Rather than enact more state laws that impose restrictions on businesses performing interstate commerce that also collect consumer data, the Alaska state legislature should encourage Congress to pass a national data privacy framework that will promote innovation while providing certainty across state borders for the regulation of data privacy.

Again, I urge you to vote against HB 159.

Sincerely,

Tom Schatz

March 17, 2022

The Honorable Rep. Matt Claman
Chair of the House Judiciary Committee
State Capitol Room 118
Juneau, AK 99801

The Honorable Rep. Liz Snyder
Vice Chair of the House Judiciary Committee
State Capitol Room 421
Juneau, AK 99801

RE: Letter in Opposition to Alaska HB 159 – Version G

Dear Representative Claman and Representative Snyder:

On behalf of the advertising industry, we oppose Alaska HB 159 – Version G ("HB 159").[1] We and the companies we represent, many of whom do substantial business in Alaska, strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, HB 159 contains provisions that could hinder Alaskans' access to valuable ad-supported online resources, impede their ability to exercise choice in the marketplace, impose prescriptive requirements that will harm businesses of all sizes and the economy, without providing countervailing consumer benefits

To help ensure Alaskan businesses can continue to thrive and Alaskan consumers can continue to reap the benefits of a robust ad-supported online ecosystem and exercise choice in the marketplace, we recommend that the legislature undertake a study of available approaches to regulating data privacy before moving forward with enacting the onerous, and in some cases, outdated provisions set forth in HB 159. As presently written, the bill falls short of creating a regulatory system that will work well for Alaskan consumers or businesses. Below we address a non-exhaustive list of areas of concern with the bill at this time.

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 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 you on further study of the proposal with an aim toward better aligning the wants of consumers with the needs of the Internet economy.

I. Alaska Should Not Model Its Approach to Data Privacy Off of Outdated and Confusing Privacy Standards

Though HB 159 appears to draw many of its provisions from the California Consumer Privacy Act of 2018 ("CCPA"), the bill does not take into account many clarifications to the CCPA that followed its initial passage. The CCPA was amended more than five times after its enactment in June

[1] HB 159 – Version G (Alaska 2022) (hereinafter "HB 159"), located here.
[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").

2018, and the California Attorney General revised the regulations implementing the law four times after initially publishing draft regulations in October 2019. Many facets of the confusing and operationally complex law are still not fully tested or fleshed out. Moreover, the CCPA is not even the most up-to-date privacy law in the state, as the California Privacy Rights Act of 2020 ("CPRA") was enacted, yet again materially amending California privacy law substantially. Further, the CPRA is a complex law that it not only relies on a yet-to-be-determined set of implementing regulations, but also a dedicated agency in California to continually interpret and update those initial regulations. Alaska should not adopt a legal regime that is outdated, confusing, or burdensome to Alaskan businesses and others operating in the state. Instead, we encourage the legislature to examine more current consumer protection standards that are available for regulating data privacy, including the Virginia Consumer Data Protection Act ("VCDPA"), before moving forward with HB 159.

As currently drafted, HB 159 also would create some of the most onerous requirements in the nation, potentially depriving Alaskans of valuable online content and services. For instance, the bill would impose onerous requirements on businesses related to basic data collection activities. The bill would require businesses to include a "Do Not Collect or Sell My Personal Information" link on their homepages that would appear to prohibit a covered business following an opt out from "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means, actively or passively receiving information from the consumer, or by observing the consumer's behavior."[3] Such a "do not collect" requirement, however, would prevent basic and vital Internet operations, including rendering a website to a visitor. This could result in many providers of online content and services to elect not to serve Alaskans, particularly given the threat of a private right of action which is included in the bill. Indeed, when the Federal Trade Commission recently opined on a related matter, it stated: "Privacy standards that give short shrift to the benefits of data-driven practices may negatively affect innovation and competition. Moreover, regulation can unreasonably impede market entry or expansion by existing companies; the benefits of privacy regulation should be weighed against these potential costs to competition."[4]

Efforts to emulate the CCPA in Alaska will significantly and disproportionately impact the ability of small and mid-size businesses and start-up companies to operate successfully in the state. A standardized regulatory impact assessment of the CCPA estimated *initial* compliance costs at 55 billion dollars.[5] This amount did not account for ongoing compliance expenses and needed resource allotments outside of the costs to businesses to bring themselves into initial compliance. Additionally, that same report estimated that businesses with less than 20 employees would need to spend $50,000 each to begin their CCPA compliance journey, and businesses with less than 50 employees would need to spend approximately $100,000 each.[6] Other studies confirm the staggering costs associated with varying state privacy standards. One report has 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.[7]

---

[3] HB 159, Sec. 45.48.940(7); Sec. 45.48.800(c)(1).

[4] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 11 (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.

[5] California Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act Regulations* at 11 (August 2019), located at https://www.tellusventure.com/downloads/privacy/calif_doj_regulatory_impact_assessment_ccpa_14aug2019.pdf.

[6] *Id*.

[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).

Alaska should reconsider implementing outdated provisions of the CCPA, that now have been supplanted, as foundational aspects of its own privacy bill.

II. Proposed Global Privacy Control Provisions Lack Reasonable Safeguards to Protect Consumer Choice

HB 159 would require businesses to "treat the use of [a] global privacy control as a valid request submitted by the consumer" to opt out of sales, sharing, and disclosures of personal information and/or categories of personal information.[8] These provisions should be subject to further study by the Alaska legislature to ensure that any global privacy control requirement includes protections to guarantee that such controls are user-enabled, rather than turned on by default by technology intermediaries. HB 159's current provisions surrounding such controls are not accompanied by sufficient safeguards to ensure a preference indicated by a setting is a true expression of a consumer's choice.

Such controls 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.[9] 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. 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.[10] 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, the global privacy control provisions should be removed from HB 159.

III. HB 159 Should Not Include Prescriptive Requirements That Add Compliance Costs Without Providing Countervailing Benefits to Consumers

In contrast to already-enacted state privacy laws, HB 159 would impose prescriptive, operationally burdensome requirements on businesses without providing commensurate protections or benefits for Alaskan consumers. For example, the bill would require downstream entities that receive personal information from businesses to notify *the business that originally collected the personal information from the consumer* and provide the downstream entity's contact information to that business.[11] This requirement, which is included in no other state privacy law, ignores the fact that downstream entities may not know which business originally collected personal information from a consumer. Moreover, this requirement provides no cognizable consumer benefit. Similarly, HB 159 would require businesses to disclose the names of sources of personal information and the names of third parties to whom they disclose personal information in response to a consumer access request.[12] These requirements could run afoul of confidentiality terms businesses maintain in contracts with their data sources and data recipients. Additionally, they would likely cause privacy disclosures to be extraordinarily lengthy and unintelligible. Alaska should refrain from including prescriptive

---

[8] HB 159, Sec. 45.48.835(b).
[9] *See,* CPRA, § 1798.185(a)(19)(A); Colorado Privacy Act, § 6-1-1313(2).
[10] *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.")
[11] HB 159, Sec. 45.48.810(a).
[12] *Id*. at Sec. 45.48.820(a)(2); 830(a)(1).

requirements such as these in its privacy bill, as such obligations would significantly complicate compliance efforts for businesses and would not benefit consumers.

IV. Broad Regulatory Authority Increases the Possibility for Divergent State Privacy Standards

As currently written, HB 159 would provide the Alaska Attorney General with broad regulatory authority.[13] Such authority would not support the development of a uniform approach to data privacy so consumers have consistent rights and businesses have predictable compliance obligations, but rather would run contrary to that goal. Under the current draft of the bill, Alaska's privacy law would have the potential to diverge even more dramatically from privacy laws in other states, as the Alaska Attorney General would be able to promulgate regulations and interpret the bill in ways that differ from privacy standards in other areas of the country. This would deprive consumers across the nation of commonality in privacy rights, and it would deny companies the regulatory reliability to enable effective compliance across the country. We therefore encourage the legislature to not include regulatory authority in any privacy legislation it considers to better ensure congruity among state standards for data privacy.

V. HB 159 Should Not Include a Private Right of Action

As presently drafted, HB 159 allows for private litigants to bring lawsuits by deeming violations of the bill to be unfair or deceptive acts or practices under the Alaska Consumer Protection Act.[14] We strongly believe private rights of action should have no place in privacy legislation. Instead, enforcement should be vested with the Alaska Attorney General ("AG"), because such an enforcement structure would lead to strong outcomes for Alaskans 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 HB 159 would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions would flood Alaska'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, including a private right of action in HB 159 would 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 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.

[13] HB 159, Sec. 45.48.195.
[14] HB 159, Sec. 45.48.890; Alaska Stat. §§ 45.50.471 – 45.50.561.

Beyond the staggering cost to Alaska 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.

VI. The Data-Driven and Ad-Supported Online Ecosystem Benefits Alaskans 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.[15] 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.[16] 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.[17] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest internet companies, which generated 34 percent.[18] The same study found that the ad-supported Internet supported 11,855 full-time jobs across Alaska, almost double the growth in Internet-driven employment from 2016.[19]

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.[20] 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 2025" if third-party tracking were to end "without mitigation."[21] 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.[22] 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.[23] 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 Alaskans' Access to Online Services and Content

---

[15] *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.
[16] *Id*.
[17] *Id*.
[18] *Id*. at 6.
[19] *Compare id.* at 121 (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 6,402 full-time jobs to the Alaska workforce in 2016 and 11,855 jobs in 2020).
[20] *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.
[21] *Id*. at 34.
[22] *Id*. at 15-16.
[23] *Id*. at 28.

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,[24] 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.[25] Publishers have been impacted 14 percent more by such reductions than others in the industry.[26] Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.[27] 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.[28] 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 must pay for most content.[29] 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.[30]

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

---

[24] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

[25] 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

[26] *Id*.

[27] *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.

[28] 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.

[29] 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.

[30] 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.

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 HB 159 would impose new and particularly onerous requirements on entities doing business in the state and would unnecessarily impede Alaska residents from receiving helpful services and accessing useful information online. We therefore respectfully ask you to reconsider the bill and instead convert it to a study so Alaskans can benefit from the legislature's careful consideration of approaches to data regulation that benefit consumers and businesses alike.

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: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP