January 15, 2021

The Honorable Sen. Reuven Carlyle
Chair of the Senate Environment, Energy & Technology Committee
233 John A. Cherberg Building
Olympia, WA 98504-0436

RE: Washington Privacy Act of 2021 (SB 5062)

Dear Senator Carlyle:

On behalf of the digital advertising industry, we provide comments on SB 5062, the Washington Privacy Act of 2021 ("WPA").[1] As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country, 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 U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. We and the companies we represent strongly believe consumers deserve meaningful privacy protections.

We also believe in the importance of maintaining a thriving Internet and information driven economy, where robust innovation drives strong economic growth, employing millions of Americans and providing transformative benefits for consumers. These objectives are not mutually exclusive. It is vital that consumer privacy legislation appropriately support these key objectives. Washington state, along with the United States as a whole and the rest of the world, has borne witness to a historic economic downturn and a significant uptick in unemployment due in large part to the COVID-19 pandemic.[2] At a time when we all face some of the most challenging circumstances in recent history, legislation that threatens to increase financial strain on companies can have the unintended effect of forcing businesses to divert important resources away from maintaining employment levels in order to address sweeping new legal requirements. We encourage the Washington legislature to carefully consider the impacts privacy legislation could have on businesses and how such impacts may trickle down to consumers if legislation is not reasonably tailored to work for both consumers and businesses in the state.

Below we provide comments on the WPA. We look forward to working with you, the Senate Environment, Energy & Technology Committee, and the legislature as a whole to refine this legislation.

---

[1] SB 5062 (Wash. 2021), located at https://app.leg.wa.gov/billsummary?BillNumber=5062&Initiative=false&Year=2021.

[2] Paul Roberts, *Is 10% unemployment a new 'normal' for Washington state?*, SEATTLE TIMES (Aug. 13, 2020), located at https://www.seattletimes.com/business/economy/new-jobless-claims-falling-in-washington-but-nearly-600000-still-on-unemployment-benefits/; *New business starts in Washington state have slowed – Coronavirus Economy daily chart*, SEATTLE TIMES (Aug. 7, 2020), located at https://www.seattletimes.com/business/new-business-starts-in-washington-state-have-slowed-coronavirus-economy-daily-chart/; *COVID-19 to Plunge Global Economy into Worst Recession since World War II*, THE WORLD BANK (Jun. 8, 2020), located at https://www.worldbank.org/en/news/press-release/2020/06/08/covid-19-to-plunge-global-economy-into-worst-recession-since-world-war-ii.

I. Enforcement of the WPA Should be Vested in the Attorney General

As presently drafted, the WPA intends to place sole enforcement authority within the purview of the state Attorney General ("AG").[3] We agree with this approach, as it would lead to strong outcomes for consumers while better enabling businesses to allocate funds to developing processes, procedures, and plans to facilitate compliance with new data privacy requirements. During the previous two legislative sessions, attempts to add a private right of action to the state's developing privacy legislation ultimately resulted in the bill failing to pass. To avoid a similar result for the WPA in 2021, we believe the bill should not be altered in any way to include a private right of action, as AG enforcement is in the best interests of consumers and controllers alike.

Adding a private right of action to the WPA would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions would flood the 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 the WPA 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 controllers 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 controllers' attempts to innovate by threatening companies with expensive litigation costs, especially if those companies are visionaries striving to develop transformative new technologies.

Beyond the staggering cost to Washington 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 keep the WPA's enforcement provision as-is and refrain from including a private right of action in the bill. An AG enforcement framework would lead to strong outcomes for consumers while better enabling controllers to allocate funds to developing processes, procedures, and plans to facilitate compliance with new data privacy requirements under the WPA.

II. The WPA's Intent Provision Could Hinder Consumer Privacy Choices and Concentrate Power in the Hands of Intermediaries

The WPA contains an intent provision that could encourage intermediary interference in consumer privacy choices.[4] The provision "encourages the state office of privacy and data protection to monitor the development of universal privacy controls that communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of their personal data."[5] In addition, the WPA requires the Washington Office of Privacy and Data Protection, in collaboration with the Office of the Attorney General, to research browser settings, extensions, and global device settings to facilitate opt out requests, deliver a report on their findings, and issue recommendations to the Governor and

[3] WPA, §§ 111, 112.
[4] *Id*. at § 2(9).
[5] *Id*.

legislature.[6] These terms would encourage the legislature to create requirements for controllers to honor controls set through intermediaries in future privacy bills or amendments. We strongly advise against including any mandate for controllers to honor controls set through intermediaries.

If the legislature were to require controllers to accept a signal or control set through a browser or other intermediary, consumers' ability to make individualized, business-by-business selections about which entities can and cannot use personal data would be threatened. These blanket controls cast a single opt out signal to every controller across the entire Internet ecosystem, thereby threatening the granular, controller-specific opt out structure set forth in the WPA.[7] Consumers could consequently lose access to a variety of online products and services they expect to receive, as a universal opt out selection would be applied to all controllers regardless of a consumer's potential desire to allow any one specific controller to engage in targeted advertising or other personal data transfer-related activities.

Controls such as these concentrate power in the hands of the intermediary or browser that provides the control. At a moment when many states are currently closely examining the problems that concentration of power can entail, the WPA's further entrenching of power in a handful of companies is problematic. Moreover, mandating that controllers must honor these intermediary-based controls could have the unintended result of turning the WPA's opt out regime into an opt in regime. After receiving a universal signal from a given consumer, with no ability to independently validate whether the choice was set by the consumer or by the intermediary, a controller would have no choice but to contact the consumer to see if they would like to opt in to sales of personal data in order to continue receiving the products and services they expect. The WPA clearly sets forth an *opt out* structure for personal data sales, targeted advertising, and profiling. It is not the intent of the draft legislation to impose an *opt in* requirement for personal data transfers. We therefore caution the legislature from taking any future actions to require controllers to honor controls set through intermediaries or browsers. Such controls hinder consumers' ability to exercise choice in the marketplace and run contrary to the WPA's intended opt out approach.

III. Minor Clarifications to the Sale Definition Will Better Serve Consumers and Provide Needed Clarity for Controllers

The WPA would provide a Washington resident with the right to opt out of "the processing of personal data concerning such a consumer for the purposes of (a) targeted advertising; (b) the sale of personal data; or (c) profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer."[8] However, the bill does not clarify how the definitions of "targeted advertising" and "sale" work together, which could create confusion in the marketplace and for consumers when it comes to opt outs.

The term "targeted advertising" under the bill covers "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preference or interests."[9] The definition of targeted advertising *excludes* essential ad operations that are imperative for the Internet to work, because such ad operations are not used to "predict [a] consumer's preference or interests."[10] These operations include ad delivery, reporting, and ad fraud prevention.

[6] *Id*. at § 116.
[7] *Id*. at §§ 103(5), 104(1).
[8] *Id*. at § 103(5).
[9] *Id*. at § 101(32).
[10] *See id*.

The definition of sale, however, does not include a similar delineation that provides cover for essential ad operations, and consequently, enables the continued functionality of the Internet.[11] Sale is defined broadly as "the exchange or processing of personal data by the controller for monetary or other valuable consideration from a third party."[12] It is unclear from this definition whether a consumer opt out from sale would cover essential ad operations that involve data exchanges – not for targeted advertising purposes – but for ad delivery, reporting, and ad fraud prevention.

We respectfully ask you to update the WPA's definition of sale to clarify this ambiguity in the legislation. Our suggested updates to the WPA's definition of sale are set forth in **Exhibit A**. We ask you to alter the definition of the term "sale" pursuant to our suggested language so it makes clear that an opt out from sale would not apply to activities that are carved out from the definition of targeted advertising as essential ad operations.

IV. The WPA Would Prohibit Controllers from Offering Consumers the Choice Between Ad-Supported Content and Fee For Content and Could Eliminate Washingtonians' Ability to Access Loyalty Programs

The WPA's terms threaten to limit publishers from giving consumers the ability to choose ad-supported, free content instead of content that is subscription-based or behind a paywall. The bill could also have drastic implications for Washingtonians' ability to access and make use of loyalty programs in the same ways as consumers in other states.

The WPA prohibits a controller from "discriminat[ing] against a consumer for exercising any of the rights contained in [the WPA], including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to a consumer."[13] This provision could have the inadvertent effect of eliminating publishers' ability to offer consumers the choice between ad-supported content and paying a fee for content. As we described in detail in Section VIII below, the ad-supported digital advertising model enables consumers to access important content, information, and services at little or no cost to them. By banning controllers from charging different prices or rates for goods or services, controllers could be limited in their ability to offer free content to consumers who want to allow transfers of personal data and participate in the ad-supported model. In the absence of ad revenue, controllers would be forced to make all consumers subscribe before allowing them to access online services or content. Consumers overwhelmingly prefer the ad-supported model to subscription-based services, and they should not be forced to pay for subscriptions to every online content or service provider due to the onerous commands of the WPA.

The WPA also places burdensome limitations on controllers' provision of loyalty programs that could ultimately eliminate the availability of loyalty, rewards, and discount programs for consumers in the state. Though the WPA does not prohibit a controller from offering consumers different prices (*i.e.*, discounts) or levels of service, it places onerous restrictions on controllers' ability to transfer personal data collected through consumers' voluntary participation in loyalty programs to "third-party controllers."[14] Due to these burdensome restrictions, controllers will be disincentivized from offering loyalty programs to Washingtonians. As a result, consumers in the state could have fewer opportunities to receive the benefits of discounts, rewards programs, and specialized services from brands and businesses. This result could have a particularly acute impact due to the economic realities of the present time, when a considerable number of Washingtonians are out of work and are struggling to make ends

[11] *Id.* at § 101(28).
[12] *Id.*
[13] *Id.* at § 107(7).
[14] *Id.*

meet. The onerous restrictions on controllers' ability to provide data obtained through loyalty programs to third-party controllers could bring an end to Washingtonians' ability to access such programs in the state.

From coffee punch cards to grocery rewards programs and beauty store points, consumers regularly and enthusiastically participate in vast and varied loyalty programs offered by controllers. These programs enable consumers to receive more tailored offers and better prices for the goods and services they regularly receive. Additionally, controllers gain from the loyalty and brand trust they receive from consumers through their participation in these programs. However, the WPA's terms limiting controllers' ability to use the personal data they may receive as a part of such loyalty programs as they make such data available to third-party controllers removes the incentive for brands and marketers to offer such programs in the first place. As a result, such terms could very well force controllers to stop offering the programs in the state.

To help ensure that Washingtonians can continue to receive the benefits of loyalty and other discount programs alongside the rest of the American public, we recommend that the legislature remove the last sentence in Section 107(7) of the WPA. We also ask the legislature to update the WPA's terms to ensure controllers are not prohibited from offering consumers with the option to access ad-supported, free content and services through the Internet.

V. The WPA's Data Protection Assessment Terms Encourage the AG to Second Guess Controllers' Privacy Governance Decisions

The WPA requires controllers to conduct and document data protection assessments ("DPAs") for a number of activities, including: processing personal data for targeted advertising, processing of sensitive data, the sale of personal data, processing of personal data for profiling when such profiling presents certain reasonably foreseeable risks, and other processing activities presenting a "heightened risk" to consumers.[15] The legislation also enables the AG to request a copy of any DPA that is relevant to an investigation and evaluate the assessment for compliance with the WPA and other laws.[16] The legislature should remove the WPA requirement to turn over DPAs to the AG upon request because it would not enhance consumer protection and would result in unreasonable scrutiny on businesses' reasonable privacy governance decisions. The requirement to turn over such assessments to the AG upon request would result in the regulator critiquing controllers' privacy practices in hindsight and second-guessing controllers' decisions based on a predisposed perspective. It would also encourage controllers to sanitize their DPAs upon creating them, thereby frustrating the usefulness of a DPA. We therefore encourage the legislature to remove the requirement to turn over DPAs to the Attorney General.

VI. The WPA's Deletion Right Should Be Harmonized With The Same Right in Other State Laws

The WPA gives a consumer the right to delete personal data "concerning the consumer."[17] This formulation of the right to delete is overly broad and is not aligned with other laws that provide similar rights to individuals in other states. Our associations strongly believe that the United States should adopt federal legislation that would set forth a single national standard to clearly define prohibited data practices that make personal data vulnerable to breach or misuse, while preserving the benefits that come from the responsible use of data.[18] To date, Congress has not enacted such a national data privacy standard. In the

[15] *Id*. at § 109(1).
[16] *Id*. at § 109(3).
[17] *Id*. at § 103(3).
[18] *See* PRIVACY FOR AMERICA, located at https://www.privacyforamerica.com/.

absence of comprehensive federal consumer data privacy and security legislation, states should work to harmonize their approaches to such laws to foster uniformity in rights and rules for consumers and businesses alike. We therefore ask the legislature to recast the right to delete in the WPA as a consumer's right to delete personal data about them that the controller has collected "from" them.

Permitting a consumer to delete any personal data "concerning" them could extend beyond information that is solely associated with the one consumer making the deletion request, thereby impacting the rights of others. For example, the WPA's present description of the right to delete could extend to information in aggregated form, which could negatively affect the utility of important research and analytics that use aggregate information to draw general conclusions and glean important insights.

In addition, other state privacy laws, such as the California Consumer Privacy Act of 2018 ("CCPA"), use different wording to describe the right to delete. The CCPA gives consumers the right to delete personal information "about the consumer which the business has collected **from** the consumer."[19] We encourage the Washington legislature to adopt the same approach to the right to delete as other states to help harmonize laws. Aligning the right to delete with the same right in other states that have enacted omnibus privacy legislation would help to minimize consumer confusion about the scope of their privacy rights and what it means to effectuate them. Additionally, ensuring the language used to describe the deletion right matches with the CCPA will help to simplify controllers' compliance responsibilities so they do not have to adopt differing approaches to deletion for individuals living in different states. To foster harmony among state privacy laws and minimize consumer confusion and frustration, we encourage the Washington legislature to mirror the CCPA's deletion right language by altering it slightly to give Washingtonians the right to request deletion of personal data about them that the controller has collected "from" them.

VII. The WPA's Appeal Process Will Create Excessive Costs and Will Not Produce Predictability

The WPA requires controllers to establish an internal process whereby consumers may appeal a refusal to take action on a request to exercise any of the rights inherent in the WPA.[20] The bill also appears to require controllers to facilitate consumers' submission of appeal records to the Attorney General.[21] Enabling consumers to appeal controllers' decisions to decline to act on rights requests for statutorily permitted reasons will force controllers to justify their lawful decisions and will not provide greater privacy protections for consumers. The requirement would also create unpredictability in businesses' execution of consumer rights requests and open businesses up to essentially litigating every consumer rights request by a Washington citizen through the appeals process. Additionally, this requirement will obligate businesses to dedicate staff and other resources to responding to appeals, a significant expense that will most acutely impact small businesses and start-up companies at a time when they are already under considerable strain due to the COVID-19 pandemic. We therefore ask you to remove the required appeal process in the WPA to foster greater certainty in businesses' fulfillment of consumer rights requests and to reduce the excessive costs associated with this requirement.

VIII. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Throughout the past three decades, the U.S. economy has been fueled by the free flow of data. One driving force in this ecosystem has been data-driven advertising. Advertising has helped power the

[19] Cal. Civ. Code § 1798.105 (emphasis added).
[20] WPA at § 105(5)(a).
[21] *Id*. at § 105(5)(c).

growth of the Internet for years by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.[22] Calculating against those figures, the interactive marketing industry contributed $1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.[23]

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. In a September 2020 survey conducted by the Digital Advertising Alliance, 93 percent of consumers stated that free content was important to the overall value of the Internet and more than 80 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.[24] The survey also found that consumers value ad-supported content and services at $1,403.88 a year, representing an increase of over $200 in value since 2016.[25]

Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. 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.[26] It is in this spirit–preserving the ad-supported digital and offline media marketplace while helping to design appropriate privacy safeguards–that we provide these comments.

* * *

[22] John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf.
[23] *Id*.
[24] Digital Advertising Alliance, *SurveyMonkey Survey: Consumer Value of Ad Supported Services – 2020 Update* (Sept. 28, 2020), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf.
[25] *Id*.
[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.

Thank you for your consideration of these comments. We look forward to working further with you on the WPA.

Sincerely,

Dan Jaffe
Group 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

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

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
202-800-0771

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

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

Exhibit A

Suggested Language for WPA dated 01/05/21

Our suggested edits to the WPA's current definition of "sale" are indicated in red below:

(25)(a) "Sale," sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

(b) "Sale" does not include the following: (i) collecting, using, maintaining, or transferring personal data as reasonably necessary to engage in delivery of an advertisement, counting and limiting the number of advertising impressions, and validating and verifying positioning and quality of ad impressions, so long as such personal data is not used for targeted advertising; (ii) the disclosure of personal data to a processor who processes the personal data on behalf of the controller; (iii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller; (iv) the disclosure or transfer of personal data to an affiliate of the controller; (v) the disclosure of information that the consumer (A) intentionally made available to the general public via a channel of mass media, and (B) did not restrict to a specific audience; or (vi) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

* * *