May 17, 2021

The Honorable Zack Fields
Co-Chair
House Labor and Commerce Committee
The Alaska State Legislature
State Capitol Room 24
Juneau, AK 99801

The Honorable Ivy Spohnholz
Co-Chair
House Labor and Commerce Committee
The Alaska State Legislature
State Capitol Room 406
Juneau, AK 99801

Via email

Dear Representatives Fields & Spohnholz:

Thank you for the invitation to address the committee.

My name is Ashkan Soltani. I am a technologist and researcher with over twenty years of experience conducting research and investigations on technology, privacy, and behavioral economics. Currently, I am a Distinguished Fellow at Georgetown Law's Institute for Technology Law & Policy, where I am part of a team that supports a wide array of state Attorneys General on privacy enforcement and policy. Previously, my work has spanned from advising and founding multiple technology companies to contributing to journalism exposing privacy and advertising tracking. I was one of the first technologists to serve at the Federal Trade Commission (FTC), and I later served as the Chief Technologist of the FTC, advising the Commision on policy and strategy pertaining to emerging technology. I also served as Senior Advisor in the White House Office of Science and Technology Policy. I was a co-author of California's new privacy laws, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), and, most recently, was a co-creator of the proposed Global Privacy Control standard, which creates a mechanism by which consumers can communicate their privacy preferences.

I'm pleased that Alaska's legislature has dedicated itself to addressing such a timely and crucial topic. Since 1972, Alaska's Constitution has enshrined the "right of the people to privacy" and charged the legislature to implement that right.[1] HB 159 is a strong and positive step toward more fully effectuating that right. I fully support HB 159, and write with the following suggestions to ensure that the legislation is as strong as possible for Alaskans.

I. Background

I worked extensively to develop, revise, and pass California's recent privacy laws: the California Consumer Privacy Act (CCPA) and the California Consumer Privacy Act (CPRA). While these laws have been the topic of much discussion, several key points often get lost in debate:

[1] Alaska Const. art. 1, § 22.

The CCPA was initially introduced as a ballot initiative in California. The ballot measure included a strong private right of action, and early discussions contemplated requiring businesses to obtain opt-in consent in order to collect or use consumer information. Before introduction, concerns about the constitutionality and effectiveness of opt-in led to scrapping it from the proposal.[2] Later, as it became clear that the ballot measure was likely to pass, we worked closely with the California legislature to draft and adopt a compromise measure, which removed the private right of action but maintained the provision which permits consumers to utilize an authorized agent or global browser setting to invoke their rights.

After the compromise CCPA passed, industry groups, including some you have heard from in this process, spent nearly two years drafting and introducing legislative amendments to weaken the law. Some of these changes were clear in their intent, while others—such as seemingly narrow definitional changes that would exempt large swathes of businesses—were more insidious.

Ultimately, because of the raft of proposed amendments and the challenge of defending the law, I and other proponents developed a new ballot initiative, Proposition 24 or Prop 24, that clarified key points of the CCPA and strengthened several sections. Most importantly, however, Prop 24, which was enacted as the California Privacy rights Act (CPRA), includes provisions that ensure that future amendments to the law are made in furtherance of the purpose and intent of the the act. While this provides flexibility for technical amendments, it prevents the kind of sandbagging that has been the hallmark of the advertising industry in state privacy debates. No longer can they simply use their resources and persistence to slowly chip away at a strong state law.

Since the passage of the CPRA, industry has changed tack. Rather than attempting to dilute California's strong protections, industry groups have attempted to encourage and pass a series of watered-down state laws in order to promote a national standard of subpar privacy protections. Simply put, industry groups intend to use state legislatures to attain their ultimate goal of weak privacy protections passed by the U.S. Congress. This is hardly a secret,[3] and calls into question the motives and objectives of national industry organizations.

This strategy has been effective. Virginia recently passed the Virginia Consumer Data Protection Act (VCDPA), a bill drafted in large part by Amazon and other large industry players.[4] Industry's influence shows: The Act contains definitions of "personal information" that exclude

[2] While there were speech concerns about opt-in consent, more important was the reality that consumers, when asked whether to opt-in, may opt in to considerably more sharing than they would otherwise intend to consent to. This, along with the constitutional concerns, led to the opt-out standard in the initial CCPA.
[3] Todd Feathers, *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*, Markup (Apr. 15, 2021), https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious.
[4] Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), https://www.protocol.com/policy/virginia-maryland-washington-big-tech.

nearly all types of behavioral advertising practices, rendering the Act functionally ineffective at staunching current privacy harms.

Alaska has a strong foundation from which to build a meaningful privacy law to protect its citizens. In the next sections, I would like to note areas of strength of the current HB 159 as well as provide constructive feedback for how the bill could be improved.

II. Positive Aspects of HB 159

HB 159 is one of the strongest pieces of draft privacy legislation in recent years. The bill is comprehensive, contains strong substantive and enforcement provisions, and provides a clear framework for protecting Alaskans' privacy.

Definitions of Pseudonymous Information

Many privacy bills contain provisions on the same or similar rights for consumers.
These typically include: consumer notice, rights to access and deletion, and consumer control. While these provisions may appear substantially similar, the protections they afford vary widely based on nuanced definitions sections. These sections often end up undermining what appear to be strong substantive provisions, rather than strengthening them.

The current draft of HB 159 avoids many of these pitfalls. For example, it contains strong substantive definitions, including "pseudonymous" information, which does not refer to individuals by name, but nonetheless permits data brokers to exchange information about individuals. This definition responds to the realities of current digital advertising practices: Most online tracking and profiling relies on "pseudonyms." These are typically numeric identifiers corresponding to an individual or a device. Importantly, these identifiers do not not refer to individuals by name. Recognizing and addressing this practice is a key step forward for Alaska.

Authorized Agents for Consumer Rights

Second, HB 159 allows consumers to exercise their rights through use of an authorized agent. This is an important provision, because it somewhat relieves consumers of the onerous task of requesting their information from every business that has received it and instead allows for market solutions to innovate new ways to manage consumer data en masse. This has the ability to develop new industry standards, similar to anti-virus software, which helps many people manage their digital safety.

Right to Information About Third Parties

Lastly, HB 159 provides consumers with the crucial knowledge of who has their information beyond the initial business that collected it. This provision was in the original CCPA ballot initiative, but did not make it into the final law. Providing consumers with this right ensures that they can identify parties that possess their data and exercise their rights to opt out or request

deletion. Without this provision, it would be significantly more difficult for Alaskans to control their data once it has been sold or shared.

III. Strengthening HB 159

While HB 159 already contains some strong substantive and definitional sections, there is also room for improvement.

Include a Global Opt-Out Control

With few exceptions, HB 159 requires consumers to opt-out of sharing for each website or digital service. This requirement is onerous, and benefits businesses, many of whom may slip through the cracks of consumers' attention. In addition to allowing consumers to rely on an authorized agent to make requests, HB 159 should allow consumers to use a global opt-out control. The CPRA allows for this type of opt out, which enables consumers to make their privacy choices one time and requires that the businesses consumers interact with honor those choices.

I have helped to develop a new specification, the Global Privacy Control (GPC),[5] that helps implement this right. The specification, which sits in a consumer's browser, has been endorsed by state officials in California, as well as U.S. lawmakers and international privacy officials.[6] Presently some 40 million consumers use a browser or extension that supports a GPC, and major publishers such as the *New York Times* and *The Washington Post* honor the GPC signal as an opt-out under the CCPA.[7] California consumers who visit these sites with a participating browser are automatically opted-out of the sale of their personal information without having to take any additional steps.

Prohibit or Limit the Use of "Dark Patterns"

HB 159 should also address so-called "dark patterns:" user interfaces that stymie or confuse consumer decision making. The CCPA took steps to reduce these manipulative design mechanisms, including by banning the use of double-negative language, limiting the ability of businesses to force consumers to scroll through lengthy privacy policies before opting out of data use, and other provisions.[8] Ensuring that businesses cannot trick or otherwise unfairly manipulate consumers, particularly when consumers are trying to invoke their rights, is a key element of any privacy bill.

Do Not Require Verified Requests for Opting Out of Data Use, Including Location

---

[5] Global Privacy Control, https://globalprivacycontrol.org.
[6] Global Privacy Control, https://globalprivacycontrol.org.
[7] *GPC Privacy Browser Signal Now Used by Millions and Honored by Major Publishers*, Global Privacy Control, https://globalprivacycontrol.org/press-release/20210128.
[8] James Vincent, *California Bans 'Dark Patterns' That Trick Users Into Giving Away Their Personal Data* Verge (Mar. 16, 2021), https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data.

The bill, when enacted, should not require consumers to submit verified requests to opt out of businesses use of their data. Verified requests for access and deletion of data are important, since those rights, if exercised fraudulently, can adversely impact the data subject. However, simply asking a business to not use personal data does not create the same risks, and does not need the same level of verification. One specific challenge is that, as described earlier, many of the ways that consumers locations are tracked rely on pseudonymous identifiers which are difficult to authenticate using a verified request. Requiring verified requests for this type of opt out simply increases the difficulty for consumers and makes it less likely they will exercise their rights. In any instance where a consumer must make a verified request, it is essential to clarify that businesses are prohibited from using any information contained in those requests other than to comply with the request, as described in CCPA section XX 1798.135(c)(6).

Update the Definition of Sale to Include "Sale and Sharing"

Drafters should consider updating the definition of "sale" to include "sharing" and other non-value exchanges. This updated language was included in the CPRA after businesses began creating "no value" exchanges in order to circumvent the initial prohibitions in the CCPA.

Regulate the Use of Data by Nonprofit Organizations

Lastly, the bill should not exempt nonprofits. While California does not include them in its regulations, nonprofit organizations often engage in the same types of harmful data practices as for-profit organizations. For instance, the national ACLU spent over five million dollars on Facebook advertising, sharing personal information on many of its users without providing them notice or any ability to opt out.[9] Despite this, nonprofits escape meaningful regulation and oversight, both federally and at the state level.

IV. Enforcement Provisions

Include Attorney General Rulemaking

In addition to the substantive changes above, HB 159 should include rulemaking authority for the Alaska Attorney General (AG). Online advertising is a technical and fast-paced industry, and it's essential that lawmakers can update rules and regulations to keep pace with business developments.

Expand Enforcement Provisions

In addition, for any privacy law to be effective, it must allow for sufficient enforcement capability. For instance, the former Attorney General of California noted that "given that we are an agency

[9] Danielle Abril, *ACLU, A Defender of Digital Privacy, Reveals that it Shares User Data with Facebook*, Fortune (Apr. 2, 2021), https://fortune.com/2021/04/02/aclu-shares-data-facebook-third-parties-digital-privacy.

with limited resources," his office would not be able to pursue every violation of the CCPA.[10] Alaska might attempt to expand the enforcement authorities in HB 159, either by permitting broader categories of private rights of action or by permitting the AG greater authority to partner with class action litigants.

Legislators might also consider additional areas of harmonization with existing provisions, such as those in CCPA and CPRA, that would enable Alaska law enforcement to partner with other key states to pursue multistate investigations. This would greatly expand the resources of both the AG and any offices with which they collaborate.

Consider Additional Fee Structures for the Privacy Account

Lastly, HB 159 establishes a "consumer privacy account" to be funded through civil penalties levied in enforcement actions. Drafters might consider expanding the revenue sources of this fund to include a revenue-based contribution from companies participating in the digital advertising ecosystem. For instance, a company could contribute based on the percentage of its revenue it receives from the sale or use of consumers' personal information. Regulations from the AG could specify how to account for "non-monetary" value a company receives from the use of data. This contribution arrangement could be expanded for companies who are required to register as "data brokers" under the new law, for instance by requiring a contribution as a percentage of total revenue.

V. Conclusion

I appreciate the opportunity to comment on the draft of HB 159. It is an excellent start to a strong privacy bill with many areas for improvement. I hope to continue to work with you as the bill progresses. Please do not hesitate to contact me with any questions.

Sincerely,

Ashkan Soltani

[10] Nandita Bose, *California AG Says Privacy Law Enforcement To Be Guided by Willingness to Comply*, Reuters (Dec. 10, 2019), https://www.reuters.com/article/us-usa-privacy-california/california-ag-says-privacy-law-enforcement-to-be-guided-by-willingness-to-comply-idUSKBN1YE2C4.