January 14, 2021

The Honorable Reuven Carlyle
Chairman, Environment, Energy and Technology Committee
Washington State Senate
233 John A. Cherberg Building
PO Box 40436
Olympia, WA 98504

Re: S. 5062, The Washington Privacy Act (2021)

Dear Senator Carlyle,

Consumer Reports[1] sincerely thanks you for your tireless work to advance consumer privacy in Washington State through the Washington Privacy Act (WPA). Though consumers in Europe and California enjoy baseline privacy protections, Washingtonians currently do not have similar basic privacy rights. The WPA would address this by extending to Washington consumers the right to know the information companies have collected about them, the right to delete that information, and the right to stop the disclosure of certain information to third parties, with additional rights for sensitive data. These protections are long overdue: consumers are constantly tracked, and information about their online and offline activities are combined to provide detailed insights into a consumers' most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

We offer several suggestions to strengthen the proposed Washington Privacy Act to provide the level of protections that Washingtonians deserve. At the very least, the WPA should be modified

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

to bring it up to the standard of the California Consumer Privacy Act (CCPA), which was recently strengthened by the passage of Proposition 24, the California Privacy Rights Act (CPRA). In particular, the CCPA as refined by CPRA takes important steps such as adding to the statute a requirement to honor browser privacy signals as an opt out (previously it was required by regulation) and removing the "right to cure" provision in administrative enforcement. The CCPA also includes authorized agent provisions so that consumers can delegate third parties to exercise rights on their behalf, which should be replicated in this bill.

Because the WPA is based on an opt-out model, like the CCPA, the deck is already stacked against consumers. Consumers have to contact hundreds, if not thousands, of different companies in order to fully protect their privacy. Making matters worse, Consumer Reports has documented that opt-out processes can be onerous, and consumers often find it difficult to locate Do Not Sell links on data brokers' homepages. In our recent study, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?,* over 500 consumers submitted Do Not Sell requests to approximately 200 companies on the California Data Broker Registry.[2] Each company was tested by at least three study participants. We found that for 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a "Do Not Sell" link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.

In some cases, the opt-out links simply weren't there; in others, the links were difficult to find. Follow-up research focused on the sites in which all three testers did not find the link revealed that at least 24 companies on the data broker registry did not have the required DNS link on their homepage. All three testers were unable to find the DNS links for five additional companies, though follow-up research revealed that the companies did have DNS links on their homepages. If consumer testers who are actively searching for DNS links have difficulty finding them on the homepage, it's hard to imagine that the everyday consumer will find them.

To help address these issues, we offer the following recommendations:

- *Strengthen data minimization:* Privacy laws should set strong limits on the data that companies can collect and share. Consumers should be able to use an online service or app safely without having to take any action, such as opting in or opting out—by including a strong data minimization requirement that limits data collection and sharing to what is reasonably necessary to provide the service requested by the consumer. A strong default prohibition on data sharing is preferable to an opt-out based regime which

[2] Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Rights Protected*, CONSUMER REPORTS DIGITAL LAB (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

relies on users to hunt down and navigate divergent opt-out processes for potentially hundreds of different companies.

- *Require companies to honor browser privacy signals as opt outs:* In the absence of strong data minimization requirements, at the very least, consumers need tools to ensure that they can better exercise their rights, such as a global opt out. We appreciate that the WPA directs the state privacy office and the attorney general to conduct a study exploring browser privacy settings to convey an opt-out signal for targeted advertising, sale, and profiling of personal data. However, CCPA regulations *require* companies to honor browser privacy signals as a "Do Not Sell" signal;[3] Proposition 24 added the global opt-out requirement to the statute.[4] Privacy researchers, advocates, and publishers have already created a "Do Not Sell" specification designed to work with the CCPA, the Global Privacy Control (GPC).[5] This could help make the opt-out model more workable for consumers,[6] but unless companies are required to comply, it is unlikely that Washingtonians will benefit.

- *Add an authorized agent provision:* WPA should also be amended to include the CCPA's "authorized agent" provision that allows a consumer to designate a third party to perform requests on their behalf—allowing for a practical option for consumers to exercise their privacy rights in an opt-out framework.[7] Consumer Reports has already begun to experiment with submitting opt-out requests on consumers' behalf, with their permission, through the authorized agent provisions.[8] Authorized agent services will be an important supplement to platform-level global opt outs. For example, an authorized agent could process offline opt-outs that are beyond the reach of a browser signal. An authorized agent could also perform access and deletion requests on behalf of consumers, for which there is not an analogous tool similar to the GPC.

- *Strengthen enforcement*: The "right to cure" provision from the administrative enforcement section of the WPA should be removed, as Proposition 24 removed it from the CCPA. We appreciate that the language has been adjusted from the previous draft to give the AG more authority to determine whether or not a violation has been "cured," but nevertheless, this "get-out-of-jail-free" card ties the AG's hands and signals that a company won't be punished for breaking the law. In addition, consumers should be able

[3] Cal. Code Regs. tit. 11 § 999.315(c) (2020).
[4] Cal. Civ. Code § 1798.135(e).
[5] Global Privacy Control, https://globalprivacycontrol.org.
[6] Press release, *Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights*, Global Privacy Control (Oct. 7, 2020), https://globalprivacycontrol.org/press-release/20201007.html.
[7] Cal. Civ. Code § 1798.135(e); §1798.140(ak).
[8] Ginny Fahs, *Putting the CCPA into Practice: Piloting a CR Authorized Agent*, DIGITAL LAB AT CONSUMER REPORTS (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8.

to hold companies accountable in some way for violating their rights—there should be some form of a private right of action.

- *Narrow preemption:* Finally, local governments are often in the best position to set rules with respect to privacy in physical locations, such as around the use of facial recognition.[9] While we appreciate that the bill preserves local privacy laws adopted before July 2020, these provisions should be narrowed to allow cities to adopt their own facial recognition laws in the future.

While we offer these suggested improvements, we also readily acknowledge that there is a lot to like about the bill. For example, we appreciate all the work that has been done over the years to develop a strong definition of "deidentified" information and to ensure that opt-out requests need not be authenticated. In important ways, the bill in print has been improved from the previous draft, such as by limiting the amount of time companies are allowed to comply with opt-out requests to 15 days (which is ample). We highlight two other noteworthy provisions in the bill that we urge you to maintain:

- *Non-discrimination.* The WPA is superior to the CCPA with respect to the non-discrimination provisions. Not only does the non-discrimination language in WPA clarify that consumers cannot be charged for exercising their rights under the law, but it makes it clear that legitimate loyalty programs, that reward consumers for repeated patronage, are supported by the law. The CCPA, in contrast, has contradictory language that could allow consumers to be charged a different price in order to protect their privacy. We appreciate the work that has been done in the WPA to ensure that privacy protections aren't just for those who can afford them.

- *Prohibition on dark patterns.* We also appreciate that you have added a prohibition on dark patterns—deceptive user interfaces that can lead consumers to take actions they didn't intend to, including to share more personal information. This bill provides important protections to ensure that opt-in consent is meaningful. Too often, companies often use dubious dark patterns to nudge users to click "OK," providing the veneer, but not the reality of, knowing consent.[10]

[9] Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.

[10] *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent*, PRIVACY INTERNATIONAL (last visited Aug. 28, 2020), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.

Contact tracing privacy

Finally, we appreciate that new sections have been added to the WPA this year to ensure that data processed in order to help address the COVID-19 crisis has additional protections. We applaud you for requiring affirmative consent to processing of this data and for the strong non-discrimination provisions. However, we recommend several tweaks to ensure that information is adequately protected. For example, the data minimization provision should be tightened, by clarifying that processing is permitted only where it is necessary to provide the service requested by the consumer, or necessary for a public health purpose. Next, given that the consent provision does much of the work of protecting consumers' privacy in this section, the definition of consent should be strengthened so that it is at least in line with the definition in Section 101(6) of the WPA. We also recommend strengthening the enforcement provisions in Section 210 as outlined above.

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Washingtonians have the strongest possible privacy protections.

Sincerely,

Maureen Mahoney
Policy Analyst

Justin Brookman
Director, Technology Policy

cc: Members, Senate Environment, Energy, and Technology Committee