January 29, 2020

The Honorable Christine Rolfes
Chair, Ways and Means Committee
Washington State Senate
311 John A. Cherberg Building
P.O. Box 40482
Olympia, WA 98504-0482

Re: SB 6281 (Data Privacy, Carlyle)

Dear Senator Rolfes:

Consumer Reports and Privacy Rights Clearinghouse sincerely appreciate your efforts to help establish privacy protections for Washington State consumers by considering the 2020 Washington Privacy Act (WPA). The bill would extend to Washington consumers key baseline privacy protections: the right to access, delete, correct, and opt out of the sale of their personal information, and additional protections for sensitive data. This bill is a marked improvement over last year's version,[1] and we urge you to consider a number of adjustments to ensure that the bill is workable for consumers and to eliminate inadvertent loopholes that companies could exploit to avoid reforming their data practices—this is particularly important in light of early bad faith responses to similar legislation, the California Consumer Privacy Act (CCPA).

This bill provides consumers clear, affirmative rights that companies must respect: the right to delete, access, and controls over the sharing of data. The bill adds new obligations for companies like data security and non-discrimination (meaning that companies can't treat you worse for exercising your rights). And in some ways, the 2020 WPA goes beyond the CCPA, such as by providing a right to correct information, and stronger protections for sensitive information.

[1] Letter from Consumer Reports et al. to The Honorable Christine Rolfes (Feb. 21, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/02/SB-5376-Privacy-Coalition-Letter-Oppose.pdf; Letter from Consumer Reports et al. to The Honorable Zach Hudgins (March 25, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/03/Privacy-Coalition-Letter-Opposing-ITED-v.-4.pdf

But there are still some potential loopholes that need to be closed up to ensure that companies can't go ahead with "business as usual" in spite of a consumer opt-out. In California, even though companies had more than a year to prepare, implementation of the CCPA, especially with respect to the opt-out, has been truly disappointing. Many companies appear to be running the same playbook as they did when Europe's GDPR went into effect. Despite the GDPR, because of a lack of enforcement to date, companies operating in Europe have been able to get away with maintaining their existing data use practices.[2]

For example, to ensure that consumers have meaningful privacy protections, the legislation should be amended in several ways:

- *Expand definition of sale*: Though the WPA's definition of sale has been expanded to cover transfers of data for valuable consideration, it's still narrow enough to exclude much (if not most) commercial data sharing. Unless the WPA is tightened up (for example, by including any sharing of data for a commercial purpose), it might not do anything to restrict these practices.
- *Clarify definition of consent*: The definition of consent should be amended to provide that consent should be separate from other permissions and long, boilerplate contracts such as end user license agreements and privacy policies. In California, for example, some companies are seeking to ignore "do not sell" instructions by claiming that consumers have assented to sale in long-form contracts they almost certainly have never read.[3]
- *Narrow exceptions*: While we sincerely appreciate that the bill requires data processing to be necessary and proportionate for the exempted activities laid out in Section 10, these provisions in some cases are both too sweeping (internal research) and vague (compatible with processing). Similarly, the data minimization provision in Section 8 is not appropriately limiting unless it restricts collection, sharing, and use to what is reasonably necessary to operate the service requested by the consumer. With respect to the exemptions for health data in Sec. 4(2)(c)(iv), it is critically important to ensure that any exception for health data be strictly limited to bona fide research, and the new language may warrant a second review to ensure that "or personal data" is not overly permissive. Similarly, the exemptions for health data in Sec. 4(2)(e) need to be clarified further to ensure that this sensitive data is appropriately protected.

---

[2] Maureen Mahoney, *Many companies are not taking the California Consumer Privacy Act seriously—the attorney general needs to act* (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.
Natasha Lomas, *Google and IAB ad category lists show 'massive leakage of highly intimate data,' GDPR complaint claims* (Jan. 27, 2019), TechCrunch, https://techcrunch.com/2019/01/27/google-and-iab-ad-category-lists-show-massive-leakage-of-highly-intimate-data-gdpr-complaint-claims/.

[3] Natasha Singer and Aaron Krolik, *Grindr and OkCupid Spread Personal Details, Study Says*, N.Y. Times (Jan. 13, 2020), https://www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html.

- *Restore the ability for consumers to exercise a global opt-out*. A bill that relies upon consumers taking advantage of opt-out rights needs some sort of mechanism to let consumers opt out of whole categories of data sharing all at once — otherwise, the opt-out rights are not scalable and workable. In California, many companies are sending consumers to multiple sites in order to exercise their preferences.[4] For this reason, the California Attorney General has issued regulations requiring companies to treat universal signals like browser headers to be binding opt-out requests.[5] An early draft of the bill included similar provisions; they should be restored in the final law, or at the very least consumers should be empowered to delegate others to exercise their opt-out rights for them. Further, we're disappointed that even the study of global opt-out technologies has been removed from this version of the bill.
- *Revise the definition of pseudonymous:* The current definition of pseudonymous allows companies to evade access, correction, and deletion rights even if those data sets could be trivially reassociated with a unique individual. The definition of pseudonymous should require that companies believe in good faith that they could not reasonably associate the data with a particular person.
- *Strengthen enforcement*: Companies' bad faith implementation of CCPA also demonstrates need for strong enforcement—particularly by more resources for the Attorney General, and private enforcement of rights. The AG needs adequate resources to defend the privacy rights of all 7 million Washington residents, and without effective enforcement, consumers will have no protection against companies who seek to violate their privacy.
- *Separate facial recognition and allow cities to pass their own laws*: Facial recognition should be handled in a different bill, given the controversy surrounding its use.[6] Additionally, the bill's preemption provisions should be narrowed to allow cities to adopt their own facial recognition laws.[7]

Further, several key provisions came under discussion at last week's hearing, and we urge you *not* to weaken protections:

---

[4] See @jasonkint, Twitter (Jan. 1, 2020), https://twitter.com/jason_kint/status/1212431443772788737.

[5] See California Department of Justice, Proposed Regulations, California Consumer Privacy Act at § 999.315(c) (Oct. 11, 2019), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf [hereinafter "AG Proposed Regulations"].

[6] Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. Times, (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, Wash. Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[7] 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/.

- *No right to cure*: "Right to cure" language would unacceptably weaken the enforcement provisions. Not only would it excessively tax the Attorney General's office—forcing it to waste time building cases that go nowhere—it lets companies get away with bad behavior until they're caught.
- *No verification for opt-outs*: Much of the data used for tracking consumers can't be tied to an individual consumer; and the CCPA pointedly does not require verified opt-outs. Companies who send fraudulent opt-out requests could invite liability under existing law, but we could support a provision that prohibits companies from sending opt-out requests unless at a consumer's direction.
- *Do not weaken the definition of deidentification*: The definition of deidentified data in the version of the bill circulated on January 10 appropriately required companies to believe in good faith that deidentified data could not be reidentified even if the controller was motivated to do so. It also matched the definition used by the Federal Trade Commission.[8] But "household" has been removed from the latest version of the bill, and it is too broad now—it creates a big loophole that companies may take advantage of to evade the law. The bill should deal with pseudonymous data in the definition of pseudonymous, not in the definition of deidentified.
- *Do not allow companies to discriminate against consumers who exercise privacy rights*: It is extremely important that any privacy law does not punish consumers who exercise their statutory rights. We have worked in good faith to allow *bona fide* loyalty programs that reward consumers for their patronage, but the law should not permit companies to charge consumers exercising their rights under the law. This is unfair to low-income consumers, who might not be able to afford to protect their privacy.

We thank you again for your work on consumer privacy, and we look forward to continuing to collaborate with you to ensure that consumers have the strongest possible legal protections to safeguard their privacy. We would be happy to discuss these suggestions further.

Sincerely,

Justin Brookman, Director, Privacy and Technology Policy
Consumer Reports

Maureen Mahoney, Policy Analyst
Consumer Reports

[8] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Fed. Trade Comm'n at 21 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Emory Roane, Policy Counsel
Privacy Rights Clearinghouse

cc: Members, Washington State Senate Ways and Means Committee