March 4, 2020

Speaker of the House Laurie Jinkins
Minority Leader J.T. Wilcox
Members of the Washington State House of Representatives
416 Sid Snyder Ave SW
Olympia, WA 98504

RE: SB 6281 – Data Privacy

Dear Speaker Jinkins, Minority Leader Wilcox, and Members of the Washington State House of Representatives,

We would like to state our appreciation for the changes made to SB 6281, the Washington Privacy Act, which was amended in the House ITED Committee last week and passed out of the House Appropriations Committee this week. While these changes do not address all of the concerns that we and many privacy, consumer advocacy, and civil liberties organizations continue to raise, this bill is stronger than the bill that passed out of the Senate. Unlike the Senate version of the bill, the amended House version makes violations of the bill enforceable under the Washington Consumer Protection Act, allows local jurisdictions to pass stronger laws on facial recognition, and adds a warrant requirement for use of facial recognition by law enforcement.

These amendments are not perfect, but they are improvements that will greatly help consumers protect their privacy. We ask the House to support these amendments and continue to work on improving the bill by removing the facial recognition provisions and the list of exemptions and loopholes that remain in the bill.

We agree with the Attorney General's Office that the version of SB 6281 that passed out of the Senate is unenforceable.

We cannot support the Senate version of the bill as it has not addressed any of the key concerns that our group, the ACLU, and other consumer and public interest groups have raised.

While different organizations have taken different positions on the bill, we share many of the same concerns. We respectfully urge the House of Representatives to:

1. **Ensure that the bill is enforceable under the Washington Consumer Protection Act and allows for consumers to be made whole by way of a private right of action.** We urge you to learn from the California Consumer Privacy Act (CCPA), which lacks a strong private right of action. As a result, compliance has been spotty because businesses are convinced that enforcement is weak. In contrast, federal privacy laws such as the Electronic Communications Act, the Video Privacy Protection Act, the Fair Credit Reporting Act, and the Telephone Consumer Protection Act and state laws such as the Illinois Biometric Information Privacy Act include provisions for private enforcement. Washingtonians must be able to enforce their rights via a private right of action, which is an essential tool to incentivize compliance with the law.[1] We, along with other privacy and consumer advocacy groups, support the House amendment that removes the prohibition on private rights of action and makes the provisions of the bill enforceable under the Washington Consumer Protection Act.

2. **Ensure that this bill does not preempt local jurisdictions from passing stronger laws on both facial recognition and data privacy**. We support the House amendment that carves out facial recognition from the preemption provision and specifies that laws already in effect are not superseded by SB 6281. We encourage the House to remove the preemption provision altogether and allow local jurisdictions to pass stronger laws on *both* facial recognition and data privacy.

3. **Close loopholes that allow companies to skirt consumer rights.** There are several places in both the Senate and House versions of SB 6281 that give companies wiggle room to ignore consumer protections, or that weaken consumer rights.

    - Both the Senate and House versions of the bill allow personal data to be collected and sold for any purpose as long as it is disclosed in the privacy policy (See Section 8(2) and (3), which tie purpose specification and data minimization to what is "reasonably necessary for the purposes for which such data are processed, as disclosed to the consumer"). While privacy policies are useful for regulators to monitor companies' compliance with their promises and obligations, few people read or understand them. People's data should only be processed to provide services they requested and to fulfill strictly operational purposes. The bill should be amended to define all other purposes as "secondary" and require affirmative, freely given consent for such uses. Consumers should not be denied goods or services if they do not consent.

[1] Adam Schwartz, You Should Have the Right to Sue Companies That Violate Your Privacy, Electronic Frontier Foundation, (January 7, 2019), https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companiesviolate-your-privacy

- Under Section 6, consumers can only opt-out of data processing for the purposes of targeted advertising, sale of personal data, or profiling in furtherance of decisions that produce legal effects. Washingtonians should have the right to exert control over their personal information and avoid processing for any secondary purposes, even if they have previously consented.

- Many of the exemptions in Section 4 for data covered by federal laws would unnecessarily weaken the privacy protections that the bill seeks to provide and confuse Washingtonians about their rights. For instance, under the Gramm-Leach-Bliley Act, consumers do not have the right to access, correct, delete, or port the data financial institutions collect about them and have only a limited ability to opt-out of their data being shared with third parties. Federal laws may also define personal information more narrowly than Washington law. When federal laws do not preempt the states from enacting stronger protections, there is no reason to exempt that data.

4. **Make risk assessments transparent and accessible.** The risk assessment process outlined in Section 9, borrowed partly from the General Data Protection Regulation (GDPR) in Europe, could be exploited in ways that harm consumers. Because the bill makes these assessments confidential, they can hide information people need to know if they are to determine if their privacy is being threatened. Absent other important protections from the GDPR, this allows companies to claim they are strong on privacy without actually having to provide evidence. The public should have access to these assessments.

5. **Hold controllers and processers accountable for the actions of third parties.** Section 10 (4) exempts a data controller or processor from responsibility for the misdeeds of a third party to whom it discloses individuals' personal data if it did not have "actual knowledge that the recipient intended to commit a violation." This allows companies to be lax about ensuring that third parties comply with data-sharing agreements and to effectively shirk their responsibilities to consumers. It would also make enforcement very difficult.

6. **Include additional protections to safeguard the personal data of teens.** The data of children under the age of 16 should also be deemed "sensitive" under Sec. 3(34) and be subject to consent requirements. This is consistent with the California Consumer Privacy Act, which provides an opt-in to the sale of information for consumers less than 16 years of age.[2] The CCPA also makes clear that actual knowledge of whether a business is selling children's data includes willful disregard of a user's age.[3] The

[2] Cal. Civ. Code § 1798.120(c)
[3] Id.

problem with including protections only for "known child[ren]" in the Washington Privacy Act is that companies may think the best practice is to avoid gaining actual knowledge in the first place.[4] This leads to the unfortunate situation where businesses are collecting personal information from children by claiming not to know whose information is being collected rather than taking reasonable steps to give notice and obtain parental consent.

7. **Remove facial recognition, and at a minimum, ensure there is a warrant for law enforcement use of facial recognition.** Facial recognition technology allows for an unprecedented expansion of the government's surveillance power. For this reason, cities and states across the country are considering or have passed moratoria and bans on facial recognition technology. Many of our organizations have urged this legislature to adopt a moratorium. While we continue to support a moratorium, we note that the amendment to require a warrant for law enforcement use of facial recognition moves this bill in the right direction.

We ask the House of Representatives to support the amendments that have passed out of the Innovation, Technology, and Economic Development and Appropriations Committees and continue working to improve the bill. We emphasize that the Senate version of the bill is unacceptable and would not provide meaningful data privacy protections for consumers. We urge you to stand strong and commit to setting a high standard for consumer protections and protecting Washingtonians' constitutional right to privacy.

Sincerely,

American Civil Liberties Union of Washington

Consumer Federation of America

Common Sense Kids Action

Electronic Frontier Foundation

Electronic Privacy Information Center

Washington Public Interest Research Group

[4] The Future of the COPPA Rule: An FTC Workshop, (Oct. 7, 2019) (Panel 1, statement of Laura Moy, Associate Professor, Director of the Communications & Technology Law Clinic, and Associate Director of the Center on Privacy & Technology at Georgetown University Law Center)