

February 20, 2020

Zack Hudgins, Chair
Committee on Innovation, Technology & Innovation
Washington State House
205A John L. O'Brien Building
Olympia, WA 40600

RE: 2SSB 6281

Dear Chairman Hudgins:

On behalf of Consumer Federation of America as well as ACLU Washington, the Electronic Privacy Information Center, the Electronic Frontier Foundation, and Privacy Rights Clearinghouse, I am appending a fact sheet to this letter outlining the major concerns that our groups have about 2SSB 6281. We ask that you include the letter and fact sheet in the record as you deliberate on this bill tomorrow.

Significant changes are needed to provide clear, fair, and enforceable rules that will strengthen individual control and require businesses to treat personal data appropriately and responsibly by:

- Strengthening individual control over the purposes for which personal information may be processed without consumers' affirmative, freely-given consent.
- Strengthening individual rights: to avoid unwanted processing, even if they have previously consented.
- Closing the many loopholes for data covered by federal laws, which would unnecessarily weaken the privacy protections that the bill seeks to provide and confuse Washingtonians about their rights.
- Making risk assessments transparent and accessible.
- Holding controllers and processors accountable for the actions of third parties to which they disclose individuals' personal data.
- Removing the facial recognition provisions of the bill.
- Strengthening enforcement by providing a private right of action and increasing the amount of maximum penalties.
- Eliminating the preemption of local privacy protections.

The test for this bill is not whether it is stronger in some respects than the California Consumer Privacy Act or the General Data Protection Regulation in Europe. It is whether it would provide meaningful, effective privacy protection for Washingtonians. 2SSB 6281 fails that test. It places the burden on individuals to avoid unwanted data practices rather than on companies to have justifiable purposes and seek consent for using their personal information. It would facilitate the use of racially biased and inaccurate facial recognition technology, and it is weak on enforcement. Your committee has already demonstrated its commitment to enacting a law that sets out clear, robust privacy rights and obligations. We applaud you for this and urge you to stand firm on strong privacy legislation.

Sincerely yours,



Susan Grant, Director of Consumer Protection and Privacy
Consumer Federation of America

ACLU Washington, Consumer Federation of America, the Electronic Privacy Information Center, the Electronic Frontier Foundation, and Privacy Rights Clearinghouse

2SSB 6281 Must Be Changed to Truly Protect Washingtonians' Privacy

February 20, 2020

Washington legislators have an historic opportunity to enact a law that protects individuals' constitutional privacy rights and will lead the way for other states. Significant changes are needed to 2SSB 6281, however, to provide clear, fair, and enforceable rules that will strengthen individual control and require businesses to treat personal data appropriately and responsibly.

1. **Strengthen Individual Control:** The bill currently allows personal data to be collected, used 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.”)¹ 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 services if they do not consent.
2. **Strengthen Individual Rights:** 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.
3. **Close the Many Loopholes:** 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 party 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 even being threatened. Absent other important protections from the GDPR, this gives companies a hollow way to proclaim

¹ Processing that violates state or federal anti-discrimination laws is prohibited, however, and processing “sensitive” data requires an opt-in.

they are strong on privacy without actually having to show what they have done to justify that claim. The public should have access to these assessments.

5. **Hold Controllers and Processors 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. **Remove Facial Recognition:** Many studies show that this technology can produce inaccurate results, often biased against people of color. There are also serious questions about how consumers can truly consent to its use, especially in public settings. In light of these concerns, Section 17 should be removed from the bill.
7. **Strengthen Enforcement:** The bill's weak enforcement provisions in Section 12 expressly prohibit any private right of action and give exclusive enforcement authority to the Attorney General's Office, making it likely that only large patterns of violations will be punished. 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 and change errant company behavior. In addition, the maximum fine per violation, \$7,500, is far too low; compare that, for instance with the GDPR's maximum fine of 20 million Euros or 4% of annual turnover.
8. **Eliminate Preemption:** Section 14 of the bill would preempt local privacy protections such as the City of Seattle's broadband privacy rule. Local entities should be able to enact stronger privacy protections than those provided by state law.

The test for this bill is not whether it is stronger in some respects than the CCPA or the GDPR. It is whether it would provide meaningful, effective privacy protection for Washingtonians. 2SSB 6281 fails that test for the reasons we have cited. It places the burden on individuals to avoid unwanted data practices rather than on companies to have justifiable purposes and seek consent for using their personal information. It would facilitate the use of racially biased and inaccurate facial recognition technology, and it is weak on enforcement, which is a critical piece of any privacy legislation. Washington legislators should enact a law that sets out clear, robust privacy rights and obligations.

We applaud Washington legislators for their commitment to protecting the privacy of their constituents and urge them to strengthen this legislation to accomplish that goal.