Data Privacy

Information Sheet on 2SSB 6281

ACLU Washington

- **Has insufficient protections:** Washingtonians deserve privacy regulations and consumer protections that are at least as meaningful as California's CCPA and Europe's GDPR, if not stronger.

- **Offers weak protections for individual consumers:** Individuals are not able to take companies that do not comply with these regulations to court. Allowing consumers to sue via an explicit private right of action would ensure that companies have a strong incentive to comply with the law. *Sec. 11.*

- **Proposes weak punishments for violations:** The maximum fine is $7,500 for each violation. These amounts are very small compared to the GDPR, which mandates a fine of up to 20 million euros ($21,598,260 as of 2/18/20 rate) or 4% of annual turnover (sales), whichever is greater. *Sec. 12*

- **Allows companies to slip through loopholes:** Your decisions should be the final decisions on what happens to your data. No company should be able to override your privacy decisions. This bill does not clearly define the only purposes for which a business can use a consumer's data, with a laundry list of exemptions allowing businesses many opportunities to override consumer wishes. Businesses should be required to only process data to provide services requested by consumers or to fulfill consumer rights.

- **Allows biased and flawed face surveillance technology without strong regulations:** 2SSB 6281 widely legitimizes the use of face surveillance without any meaningful restrictions, and importantly, does not allow historically impacted communities to decide if and how the technology should be used. We need to press pause on face surveillance, not promote its expansion. *Sec. 17*

    - **Face surveillance is not ready for primetime:** Research shows that current facial recognition systems are rife with race and gender biases. We must press pause on face surveillance because it isn't ready for prime time, cannot be detected, and is already being adopted by government agencies making decisions that impact people's rights and lives.

    - **Face surveillance testing does not produce accountability:** Testing provides transparency, but not accountability. This bill requires access to a means to test the software (API or some other technical capability) but the bill does not require that any bias found by testing be resolved.

    - **"Meaningful human review" is not clearly defined:** 2SSB 6281 requires companies to ensure that decisions involving use of facial recognition services that impact consumers be subject to "meaningful human review" but does not define what qualifies as "meaningful." *Sec. 3*

    - **Human review does not necessarily fix system bias:** The humans reviewing decisions made by automated decision-making systems are subject to bias, too.

    - **Deprives targeted communities of the power to decide:** Communities pay the price when we beta test face surveillance on them. Therefore, communities that have been frequent targets of surveillance including Black religious and community leaders; LGBTQ+ activists; Muslim and Sikh Americans; and Japanese Americans must be at the table to discuss whether face surveillance is used, not just how it is used.

- **Prevents stronger local rules:** This bill prevents local jurisdictions from enacting their own stronger data privacy and face surveillance protections, taking away power to decide what is appropriate for their local communities. Washington should set a floor for individual privacy rights, not a ceiling. *Sec. 14*