CENTER FOR DEMOCRACY & TECHNOLOGY

February 26, 2019

The Honorable Christine Rolfes, Chair
Members of the Senate Ways & Means Committee
311 J.A. Cherberg Building
P.O. Box 40466
Olympia, WA 98504-0466

RE: Necessary Changes to the Washington Privacy Act (Substitute SB 5376)

Dear Chair Rolfes:

The Center for Democracy & Technology[1] writes to express serious concerns with Substitute SB 5376. We would encourage the Committee to not advance this legislation further absent significant changes. This is a pivotal moment for privacy rights across the United States, but in the rush to address public concerns about data privacy and commercial business practices, we should not enact laws that will only enshrine the status quo and leave too much flexibility to exploit personal information and skirt obligations to protect privacy.

Unfortunately, as currently amended, SB 5376 does just this. The positive elements in the bill are overshadowed by significant exceptions that undermine the bill's stated aims. Too many companies have shown that they should not be trusted to regulate themselves when it comes to respecting our privacy, but the current version of SB 5376 effectively asks us to trust them once more.

When SB 5376 was introduced, CDT identified several key concerns:

- The broad safe harbor for de-identified data;
- The reliance on corporate risk assessments for restricting data collection, use, and sharing;
- The need to provide additional resources for meaningful enforcement; and
- The proposed rules for public and private use of facial recognition technologies (FRTs).[2]

Unfortunately, rather than addressing these issues, subsequent revisions to the bill have introduced new loopholes that drastically limit the scope of the bill's privacy protections. In fact, Substitute SB 5376 has weakened or eliminated many of the protections we initially

[1] The Center for Democracy & Technology is a non-profit, non-partisan technology advocacy organization based in Washington, D.C., that works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security online.

[2] Joseph Jerome, *The Washington Privacy Act Raises Important Considerations for Comprehensive Privacy Proposals*, Ctr. for Democracy & Tech. (Feb. 07, 2019), https://cdt.org/blog/the-washington-privacy-act-raises-important-considerations-for-comprehensive-privacy-proposals/.

highlighted as positive aspects of the proposal. As presently drafted, Substitute SB 5376 is a privacy proposal akin to a wolf dressed in sheep's clothing.

First, many privacy-invasive business activities are not captured within the scope of Substitute SB 5376. We have already explained how the initial proposal's broad exception for de-identified data was an invitation for corporate mischief,[3] but Substitute SB 5376 adds to this a strong presumption that any data processing activity for "businesses purposes" is permissible.

Certainly, companies should be able to collect and use data to fulfill a transaction, but Substitute SB 5376's list of business purposes extends far beyond the basic operational needs of businesses. It includes product development, online ad tracking, and other uses that may be beneficial to companies but are hardly essential excuses to use Washingtonian's personal information. Furthermore, Section 3(3) specifically defines a business purpose to include any "other notified purposes," which will double down on the failed notice-and-choice regime that currently governs online privacy practices.

While the initial draft of SB 5376 relied on regular risk assessments to govern data processing activities, Substitute SB 5376 Section 8(4) makes clear that there are no limitations on data collection and use for "business purposes." The only exception to this is where sensitive data is involved, but even there, processing is permitted through the use of "appropriate administrative and technical safeguards." These provisions combine to give businesses carte blanche to use data in ways that upset consumer expectations; by enshrining this sort of flexibility into law, the Washington Privacy Act may make our current privacy problems worse.

Second, we reiterate that reliance on company-directed risk assessments is, frankly, a risky way to protect Washingtonian's privacy. Substitute SB 5376 does not tell companies what risks they must consider when processing data. Companies tend to have a narrow conception of privacy risk, but as the National Institute for Standards & Technology (NIST) has acknowledged, privacy risks exist beyond economic loss and include diminished autonomy and self-determination, discrimination, and generalized loss of trust.[4] Even identifying a list of risks, however, does not provide clear direction to companies as to what they must then do.

Identifying a list of risks, however, does not provide clear direction to companies as to what they must do to mitigate or avoid them altogether. Absent a firm set of legislative rules, the NTIA's calls for risk management would give businesses considerable discretion to determine what risks individuals may assume. This is why CDT has proposed privacy legislation that *limits*

[3] *Id.* The challenge of de-identification has been discussed at length by privacy experts, Arvind Narayanan and Ed Felton. *See* Arvind Narayanan & Ed Felton, *No silver bullet: De-identification still doesn't work* (2014), *available at* https://freedom-to-tinker.com/2014/07/09/no-silver-bullet-de-identification-still-doesnt-work/.

[4] Sean Brooks et al., NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems 10 (Jan. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. *See also* Intel Privacy Legislation Discussion Draft, Section 3 (Nov. 5, 2018), *available at* https://usprivacybill.intel.com/legislation/, which suggests psychological harm, inconveniences and lost time, and other reputational harms could inform a risk assessment.

certain data processing activities where not required for a product, service, or function requested by an individual.

Enforcement remains inadequate. Once companies engage in their mandated risk assessments, they essentially exist as justification until the Attorney General comes calling. Substitute SB 5376 is operating under the presumption that the Washington Attorney General will be able to police companies data practices by requesting and reviewing these risk assessments over time. The reality is that until there is an outward facing privacy violation such as a large data breach, the capacity of the Attorney General to monitor invasive data uses will be limited.

Even assuming a company engages in their mandated risk assessment, what grounds will the Attorney General have to overturn such as assessment? Because the scope of personal information in the law has been so narrowed, companies can operate under the fiction of using de-identified or otherwise non-identifiable data. If this is well-documented as part of the company's assessment, the Attorney General may be at a loss as to how to make a case. In any event, Substitute SB 5376 also includes a generous provision that permits companies to cure certain violations of the law. We would question how this dynamic can lead to meaningful enforcement as practical matter.

Finally, Substitute SB 5376's commercial facial recognition protections are now nonexistent. Previously we highlighted concerns with how the Washington Privacy Act dealt with private-sector use of facial recognition technologies (FRTs) in public spaces.[5] Specifically, while the bill continues to propose a general requirement that consent be obtained prior to the use of narrowly-defined "facial recognition," this is completely undermined by embracing a notion of implied consent simply through a store's mere placement of some signage suggesting the use of FRTs. Merely walking into a store cannot be said to imply an individual's consent to have their face tracked, analyzed, and characterized, or verified against some database of images.[6]

As problematic as this is, the initial proposal also mandated that businesses provide some mechanism to opt-out of this tracking. Alarmingly, Substitute SB 5376 removes this requirement. This is not even in line with existing corporate best practices around facial recognition,[7] and makes any notion of implied consent meaningless.

--

[5] Jerome, *supra* note 2.
[6] Joseph Jerome, *Face Recognition Principles are a Step Forward But Congress Needs to Act*, Ctr. for Democracy & Tech. (Sept. 21, 2018), https://cdt.org/blog/face-recognition-principles-are-a-step-forward-but-congress-needs-to-act/.
[7] Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications (Sept. 2018), https://fpf.org/wp-content/uploads/2018/09/FR-Final-doc1_publish.pdf ("Exemptions to the requirement for express, affirmative consent may be in a use case that does not require consent, or in a limited set of circumstances where opt-out consent is sufficient.").

CENTER FOR DEMOCRACY & TECHNOLOGY

The Washington Privacy Act has been portrayed as including the best parts of the EU General Data Protection Regulation. The reality is that Substitute SB 5376 incorporates elements of and definitions from that comprehensive regime without putting in place the requirements or enforcement mechanisms to achieve its larger aims. (Unfortunately, provision addressing "automated profiling" where the initial SB 5376 actually built on the GDPR have been removed in the substitute proposal.)

The end result is a privacy proposal that will not protect individual's interests in their data, and we urge you to amend Substitute SB 5376 to provide both clarity and needed privacy protections.

Please do not hesitate to reach out with any questions at nduarte@cdt.org.

Sincerely,
Natasha Duarte
Policy Analyst, Privacy & Data Project
Center for Democracy & Technology