CENTER FOR DEMOCRACY & TECHNOLOGY

March 21, 2019

The Honorable Zack Hudgins, Chair
Members of the House Innovation, Technology & Economic Development Committee
205A John L. O'Brien Building
P.O. Box 40600
Olympia, WA 98504-0600

RE: OPPOSE -- Recommended Changes to the Washington Privacy Act (HB 1854 ITED v. 4)

Dear Chair Hudgins:

The Center for Democracy & Technology[1] has written previously[2] to express our concerns about and recommendations for improving the Washington Privacy Act. While we cannot support this proposal as currently drafted, we write to recommend three changes that could significantly improve the scope and coverage of HB 1854.

First, the definition of "business purpose" in Section 3(3) is overbroad and undermines the intent of the law. Certainly, companies should be able to collect and use data to fulfill a transaction, but the current list of business purposes permits activities far beyond the basic operational needs of businesses.

We would recommend the definition of "business purpose" be modified as follows:

> "Business purpose" means the processing of personal data for the controller's or its processor's operational purposes~~, or other notified purposes~~, provided that the processing of personal data must be ~~reasonably~~ necessary and proportionate to achieve the operational purposes for which the personal data was collected or processed ~~or for another operational purpose that is compatible with the context in which the personal data was collected~~.

Second, the definition of "deidentified data" in Section 3(10) remains overbroad. The current definition neither matches the Federal Trade Commission's existing "three-part" test for deidentifying data nor encourages strong deidentification procedures. This is especially

[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] *See* 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/; Letter from CDT re: Necessary Changes to the Washington Privacy Act (Feb. 26, 2019), *available at* https://cdt.org/files/2019/02/CDT-Letter-re-Washington-Privacy-Act-S_SB5376-1.pdf.

problematic because it creates a new standard through which business entities can avoid meaningful privacy rules.

We would recommend the definition of "deidentified data" be modified as follows:

> "Deidentified data" means:
>
> 1. Data that cannot be linked to a known natural person without additional information **not available to the controller** ~~kept separately~~; or
> 2. Data (i) that has been modified to a degree that the risk of reidentification is small **as determined by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for deidentifying data**, (ii) that is subject to a public commitment by the controller not to attempt to reidentify the data, (iii) to which ~~one or more~~ enforceable controls to prevent reidentification has been applied. Enforceable controls to prevent reidentification may include ~~legal,~~ administrative, technical, or contractual controls.

Alternatively, we might suggest simply adopting the FTC's formulation for deidentified data that requires companies to (1) take reasonable measures to ensure that the data is deidentified; (2) publicly commit to not attempt to reidentify it; and (3) prohibit downstream recipients by contract from reidentifying data.[3]

Third, because the Washington Privacy Act largely relies on corporate risk assessments to protect individuals' privacy, it should include a list of privacy risks that companies are required to consider. We have written previously about deferring to corporate judgment about what risks to subject individuals to, but the legislature should still provide guidance to ensure companies do not take an overly narrow view of what constitutes privacy risk.[4]

We would recommend a definition of "privacy risk" be added to Section 3 along these lines:

> "Privacy risk" means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to:
>
> 1. Direct or indirect financial loss or economic harm;
> 2. Physical harm;
> 3. Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;

---

[3] *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.

[4] *Compare* 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/, *with* Joseph Jerome, *GDPR: Avoiding Harms and Expanding Risk*, Ctr. for Democracy & Tech. (May 24, 2018), https://cdt.org/blog/gdpr-avoiding-harms-expanding-risk/.

4. Significant inconvenience or expenditure of time;
5. Adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;
6. Stigmatization or reputational harm;
7. Disruption and intrusion from unwanted commercial communications or contacts;
8. Price discrimination;
9. Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly:
    1. Alters that individual's experiences;
    2. Limits that individual's choices;
    3. Influences that individual's responses; or
    4. Predetermines results; or
10. Other adverse consequences that affect an individual's private life, including private family matters, actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used.[5]

Thank you for your consideration of these changes.

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

[5] This definition is taken from a Intel U.S. privacy proposal discussion draft, *available at* https://usprivacybill.intel.com/legislation/. CDT does not endorse this definition but has supported a broad understanding of privacy risk. See FTC Informational Injury Workshop P175413 — Comments (Oct. 30, 2017), *available at* https://cdt.org/insight/ftc-informational-injury-workshop-p175413-comments/.