ELECTRONIC FRONTIER FOUNDATION

January 22, 2020

The Honorable Reuven Carlyle
State Capitol
233 John A. Cherberg Building
Olympia, WA 98504-0436

Re: S.B. 6281-OPPOSE

Dear Sen. Carlyle,

Thank you for working to improve the privacy of Washingtonians. I attended Roosevelt High School (class of '75), and I still have family in Laurelhurst and Ballard. The changes in Seattle in the last 45 years have been amazing, and reflect the impact of companies like Microsoft and Amazon. Tech has brought great innovation to the world, but at a significant cost—it has not preserved or improved privacy for ordinary Americans, and requires a strong check to stop the erosion of this valuable right. EFF commented on S. 5376 in 2019, and we appreciate the opportunity to provide input as the Washington legislative process proceeds in this short session.

We agree with other privacy advocates that your current bill both possesses and lacks certain features that are important to EFF. We appreciate your willingness to hear from the privacy community, but must oppose this bill as currently written because of its treatment of private rights of action, risk assessments, and the inclusion of facial recognition regulations.

The current version of the bill, in Section 11**,** expressly rejects private rights of action. EFF strongly supports the right of ordinary people to bring civil actions against entities that harm their privacy or other rights.[1] People rightly can sue over product defects, car accidents, breach of contract, or injuries to reputation—they do not have to wait for the state attorney general to bring actions on their behalf in any of these instances. Why should privacy harms be an exception? Private rights of action provide a valuable enforcement tool for everyday people, and also ensure that companies face real consequences for privacy harms.

Similarly, we encourage you to rethink the way this bill treats data protection assessments in section 9 of your bill, adapted from the GDPR. EFF does not categorically oppose such assessments, but we also do not view them as being useful in protecting consumers without being integrated into a serious regulatory compliance scheme that includes accessibility to the public. The GDPR includes risk assessments as one of many tools to curb unnecessary data collection and unexpected data use. As written in your bill, the risk assessment process could be exploited in ways that harm consumers, by hiding information they need to know if their privacy is even being threatened.

[1] https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy

First, it is unclear whether companies genuinely must produce such assessments. Section 9 seems to say so, but from our reading of the text, nothing actually turns on the assessment. Second, no consumer can know about the assessment because your bill declares it "confidential" in Sec. 9(3). Even the Attorney General may only request disclosure of an assessment if it "is relevant to an investigation conducted by the attorney general," in Sec. 9(3). This goal of keeping consumers in the dark is amplified by Sec. 9(4), which appears to ensure that assessments conducted for compliance with other laws (presumably the GDPR) are also confidential. Third, we are dismayed that the requirements for assessments under 9(2) seem to asymmetrically favor potential benefits of personal data processing and not its risks. For instance, that section expressly mentions direct and indirect benefits to controller, consumer, stakeholders, and the public while the only risks that matter are to the consumer. Yet it is abundantly clear that, at the very least, risks to privacy and civil liberties occur at a societal level as well as a group level, and not just to individuals.

Privacy legislation that protects consumers should provide more true transparency for consumers and empower them with the information they need to hold companies accountable. EFF fears that the assessment process will be something that companies loudly spend money on that lets them talk about how much they're committed to privacy, without ever having to show their work.

Finally, EFF also dislikes the facial recognition aspects of the bill. We have worked with civil liberties groups and leading face recognition scholars across the country to educate communities about the risks and harms of government use of face recognition technologies.[2] The issues around facial recognition are complex, and it is pure fact that we as a nation are grappling with its use. A number of cities and states around the country have passed or are seriously considering bans on face surveillance. They have asked their legislators not to endorse the use of this technology in communities that have not had adequate time to explore the harms and privacy tradeoffs of this powerful technology. A recent story from the New York Times[3] makes quite clear that there is no hermetic separation between commercial and government use of FR technology. We think that a path forward will be considerably easier if FR is addressed in a separate bill.

This short letter cannot, of course, address all of the issues that EFF has with your bill. We hope to discuss some of these other issues, such as "pseudonymous" information, at a later time.

[2] https://www.eff.org/deeplinks/2019/12/year-fight-against-government-face-surveillance
[3] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

We look forward to having further conversations with you about your bill, and thank you for the opportunity to provide feedback. Please feel free to contact either myself at tien@eff.org or Legislative Activist Hayley Tsukayama at hayleyt@eff.org at any time.

Sincerely,

Lee Tien

Senior Staff Attorney
Adams Chair for Internet Rights
Electronic Frontier Foundation
(415) 436-9333 x 102