Innovation, Technology, and Economic Development Committee
House of Representatives, State of Washington
205A John L. O'Brien
P.O. Box 40600
Olympia, WA 98504-0600

March 21, 2019

Dear Mr. Chair and Members of the House Innovation, Technology, and Economic Development Committee,

The Future of Privacy Forum respectfully submits the following comments regarding the proposed Washington Privacy Act, Senate Bill 5376 as amended (the Bill).[1] We take a "neutral" position regarding the Bill.

FPF is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF is supported by the privacy officers of more than 150 companies and by leading foundations, with an advisory board of academic, civil society, and industry members.[2] FPF recently established an office in Seattle, which is the center for our Smart Communities project.[3] This effort brings together privacy leaders at municipalities around the country who are implementing smart city projects in order to help them develop strong data protection frameworks.

We write to:

- *Offer further engagement on meaningful regulation of facial recognition technologies*. In recent years, FPF has published resources on the distinctions between related technologies, including facial detection, facial characterization, and facial recognition. In light of the complexity involved in crafting meaningful regulation of biometric technologies, we strongly recommend that the issue be resolved by a separate, future regulatory effort.
- *Recommend expert resources on data de-identification.* Most personal information exists on a continuum of identifiability. While some data is firmly linked to an individual or provably non-linkable to a person, significant amounts of data exist in a gray area -- obfuscated but potentially linkable to an individual under some circumstances. Wise policies take account of this spectrum of identifiability and provide incentives for companies to de-identify data using technical, legal, and administrative measures.
- *Recommend greater clarity on the intersection of the Bill and the complexities of education-related privacy concerns.* For the benefit of schools, administrators, and education technology ("edtech") vendors, FPF recommends clarifying several key

[1] Washington Privacy Act, 2SSB-5376 (H-2436.1), 66th Leg. (Wash. 2019), https://app.leg.wa.gov/committeeschedules/Home/Document/201663.
[2] The views herein do not necessarily reflect those of our supporters or our Advisory Board.
[3] *See* Smart Communities, Future of Privacy Forum, https://fpf.org/issues/smart-communities/.

points of the Bill that are applicable to education and student privacy, including: edtech vendors' obligations under the Bill (if any) when they act solely on behalf of public schools or districts, and whether students are considered "consumers" while acting in an educational context.

A core tenant of FPF's mission is the promotion of academic and technical expertise, particularly when lawmakers and regulators take steps to address consumers' privacy concerns.[4] We hope that our comments below and the associated resources are helpful to the important, ongoing discussion regarding consumer privacy in the State of Washington.

1. Facial recognition

We commend the Bill as amended for recognizing the privacy implications of facial recognition as a uniquely sensitive data processing activity, and for incorporating more robust protections. Nevertheless, there remains significant debate within government, industry, and civil society about issues fundamental to the appropriate regulation and use of facial recognition technologies, such as meaningful consent, safeguards against discrimination, and concerns about bias, profiling, and automated decision-making. In light of the complexity involved in crafting meaningful regulation of biometric technologies, we strongly recommend that the issue be resolved by a separate, future regulatory effort.

FPF would be pleased to engage further with the Committee on this important issue. In recent years, FPF has published several resources on facial recognition, which we believe would be helpful in guiding this Committee's work. These resources were developed in conjunction with both industry representatives and advocacy organizations and represent a principled and practical approach to the responsible use of facial recognition technologies.

- Our graphic *Understanding Facial Detection, Characterization, and Recognition Technologies*[5] depicts the distinctions between related facial systems, including facial detection, facial characterization, and facial verification and identification systems, and how companies may use these different technologies while mitigating or avoiding privacy risks. We hope that this guidance will help this Committee more clearly define and address the technologies addressed in this bill

[4] *See, e.g.* Privacy Papers for Policymakers, Future of Privacy Forum, https://fpf.org/privacy-papers-for-policy-makers/ (highlighting annual privacy scholarship that is useful to policymakers); Digital Data Flows Masterclass, Future of Privacy Forum, https://fpf.org/classes (providing technical expertise on topics of interest to data privacy law and policy).
[5] Future of Privacy Forum, Understanding Facial Detection, Characterization and Recognition Technologies (2018), https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf.

(such as facial recognition and facial characterization) and address the different levels of privacy risks associated with each.

- Additionally, FPF's *Privacy Principles for Facial Recognition Technology in Consumer Applications*[6] describes seven core privacy principles that address public concerns surrounding personally identifiable information (PII) (templates of individual faces) collected by these systems. These Principles were developed in partnership with system providers, users, and consumer protections advocates for use by companies as a resource for the development, refinement, and implementation of facial recognition technology in commercial settings, and we believe provide an appropriate baseline for consumer protection legislation.

2. Data identifiability and personal information

In addressing the privacy implications inherent in defining personal information and de-identified data, lawmakers should be aware of the growing body of technical and legal literature on de-identification that inform current privacy law, policy, and practice. FPF seeks to identify and develop leading practices on this issue and has significant experience working with experts on a range of modern de-identification practices. Additionally, FPF has developed educational materials and programs on state-of-the-art approaches to privacy-preserving data use and sharing, such as differential privacy and secure computation.[7]

According to the Federal Trade Commission (FTC), data are not "reasonably linkable" to individual identity to the extent that a company: (1) takes reasonable measures to ensure that the data are de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data (the "Three-Part Test").[8] Commercial entities within the FTC's jurisdiction operate within this legal framework and take this definition into account.

Nonetheless, determining when data is "reasonably linkable" to an identified or identifiable person is a complex technical and legal question. Most personal information exists on a continuum of identifiability. While some data is firmly linked to an individual or provably non-linkable to a person, significant amounts of data exist in a gray area -- obfuscated, but potentially linkable to an individual under some circumstances.[9] We hope

---

[6] Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications (2018), https://fpf.org/wp-content/uploads/2018/09/FR-Final-doc1_publish.pdf.
[7] Digital Data Flows Masterclass, Future of Privacy Forum, https://fpf.org/classes-archives/.
[8] Protecting Consumer Privacy in an Era of Rapid Change, Federal Trade Commission (2012), at 21, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[9] *See* A Visual Guide to Practical De-Identification, Future of Privacy Forum (2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Visual-Guide-to-Practical-Data-DeID.pdf and its accompanying academic work; Jules Polonetsky et al., *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification*, 56 Santa Clara L. Rev. 593 (2016),

our resources in this field can be of assistance to the Committee and are available to engage further.

3. Education data

FPF has significant expertise working with stakeholders at the intersection of privacy and education. FPF's Education Privacy team has testified before Congress[10] and the Federal Commission on School Safety,[11] was invited to speak at the 2017 FTC and U.S. Department of Education workshop on "Student Privacy and EdTech," and publishes extensive resources for parents, students, educators, edtech vendors, practitioners, and policymakers.[12] FPF also co-founded the Student Privacy Pledge, a self-regulatory framework that safeguards student privacy regarding the collection, maintenance, and use of student personal information.[13]

As a threshold issue, we recommend clarifying the categorization of companies working on behalf of government entities. Schools frequently contract with edtech companies to help them manage student data, carry out school operations, and support instruction and learning opportunities.[14] These companies range from some of the largest technology companies in the world to start-ups created by teachers who wanted to better serve their students.

Currently, the Bill defines a "controller" as "the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data" and a "processor" as "a natural or legal person that processes personal data on behalf of the controller." However, the "natural or legal person" language used to define controllers and processors omits the wider scope of entities that are considered "third parties" under the Bill, including "a natural or legal person, **public authority**, **agency**, or **body**…" It therefore appears that public schools, which are generally categorized as public agencies, are not considered to be controllers, and as a result their vendors are not processors. Such ambiguity is likely to cause both schools and edtech vendors confusion as they consider how to comply with any new obligations as a result of the Bill.

---

https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2827&context=lawreview.

[10] FPF Testifies Before Congress on Promoting and Protecting Student Privacy, FERPA SHERPA (May 18, 2018), https://ferpasherpa.org/fpf1/ (last visited Mar. 8, 2019).

[11] FPF Testifies Before Federal Commission on School Safety, FERPA SHERPA (July 11, 2018), https://ferpasherpa.org/fpf-testifies-before-federal-commission-on-school-safety/ (last visited Mar. 8, 2019).

[12] The Education Privacy Resource Center, FERPA SHERPA, https://ferpasherpa.org/ (last visited Nov. 9, 2018).

[13] 350 leading education technology companies have signed the pledge. *See* The Student Privacy Pledge, Future of Privacy Forum & The Software & Information Industry Association (2019), https://studentprivacypledge.org/ (last visited Mar. 8, 2019).

[14] The US Department of Education refers to edtech vendors as "vendors and other third party providers who are developing, or selling educational technology apps or services that utilizes or collect or uses Students' Personally Identifiable Information." *BY AUDIENCE: Education Technology Vendors*, US Department of Education, https://studentprivacy.ed.gov/audience/education-technology-vendors (last visited Mar 8, 2019).

Similarly, it is not clear whether a student acting only in an educational context would be considered a "consumer" under the Bill. A consumer is defined as a "natural person who is a Washington resident acting only in an individual or household context," and not "a natural person acting in a commercial or employment context." However, students engaging in educational activities at school would not clearly fall into any of the categories described in the Bill. Whether students' educational activities are subject to the protections of the Bill could have a substantial impact on the ability of schools and edtech vendors to deliver educational services in Washington.

In the context of K-12 education, many edtech vendors process student data on behalf of schools or school districts. Under the federal law FERPA, schools and school districts must maintain direct control over data they share with third parties without parental consent.[15] This means that an edtech provider receiving student data under this exception is only allowed to use, disclose, or retain data as allowed by the school or school district. Furthermore, Washington passed a strong student privacy law[16] in 2015 that requires vendors to implement safeguards and provide clear notices designed to protect student privacy.

Overall, we recommend clarifying how education-related activities are addressed within the framework of the Bill. Given the existing backdrop of privacy-protective legislation both at the federal level and in Washington, further clarity will help bring regulatory certainty for schools, school districts, school administrators, and edtech vendors who regularly facilitate data use and protect student privacy while providing educational products and services.

Additional Resources

Finally, Future of Privacy Forum has published a broad range of technical, legal, and policy analysis on many commercial privacy issues. Below are a few highlights from recent months (for more visit www.fpf.org):

- *The Internet of Things (IoT) and People with Disabilities.* In January 2019, FPF published The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions, a report that examines the nuances of privacy considerations for people with disabilities using IoT services and provides recommendations to address privacy considerations, which can include transparency, individual control, respect for context, the need for focused collection and security.[17]

[15] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.
[16] Wash. Rev. Code § 28A.604 (2019) https://app.leg.wa.gov/RCW/default.aspx?cite=28A.604.
[17] Future of Privacy Forum, The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions (Jan. 31, 2019), https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf.

- *Artificial Intelligence and Machine Learning (ML)* -- In October 2018, FPF released the *Privacy Expert's Guide to AI and Machine Learning*, a guide for non-programmers to understand the technological basics of AI and ML systems, and to address privacy challenges associated with the implementation of new and existing ML-based products and services.
- *Digital Data Flows "Masterclass" Series* -- In October 2018, FPF launched a "Masterclass" series for U.S. and European regulators and staff who are seeking to better understand the data-driven technologies at the forefront of data protection law & policy. The program features experts on machine learning, biometrics, connected cars, facial recognition, online advertising, encryption, and other emerging technologies.[18]
- *Non-HIPAA Health Data.* In July 2018, FPF published Privacy Best Practices for Consumer Genetic Testing Services,which provides a privacy policy framework for the collection, protection, sharing, and use of genetic data by consumer genetic and personal genomic testing companies.[19] FPF also released Best Practices for Consumer Wearables and Wellness Apps and Devices, a detailed set of guidelines that provide practical privacy protections for consumer-generated health and wellness data.[20]

We hope these comments and resources will be useful to the legislative process in the State of Washington, and look forward to engaging further on these important issues.

Sincerely,

Kelsey Finch
Policy Counsel
Future of Privacy Forum
PO Box 14051
Seattle, WA 98144

Tyler Park
Education Privacy Policy Fellow
Future of Privacy Forum
1400 I St. NW, Ste 510,
Washington, DC 20005

Brenda Leong
Senior Counsel &
Director of Strategy
Future of Privacy Forum
1400 I St. NW, Ste 510,
Washington, DC 20005

[18] Digital Data Flows Masterclass, Future of Privacy Forum, https://fpf.org/classes/.
[19] Future of Privacy Forum, Privacy Best Practices for Consumer Genetic Testing Services (2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.
[20] Future of Privacy Forum, Best Practices for Consumer Wearables and Wellness Apps and Devices (2016), https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf.