FUTURE OF PRIVACY FORUM

1400 Eye Street NW, Suite 450, Washington, DC 20005 | 202-768-8950 | fpf.org

Ways & Means Committee
Senate, State of Washington
311 J.A. Cherberg Bldg.
P.O. Box 40466
Olympia, WA

February 27, 2019

Dear Madam Chair and Members of the Committee,

The Future of Privacy Forum respectfully submits the following comments regarding the proposed Washington Privacy Act, Senate Bill 5376 (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:

- *Commend the sponsors for addressing a broad set of individual data protection rights.* While FPF supports a baseline federal privacy law, states that do advance legislation should do so in ways that provide consumers with comprehensive protections, in line with the Fair Information Practice Principles (FIPPs) and the General Data Protection Regulation (GDPR).
- *Observe that risk assessments can play an important role in protecting consumer privacy.* Leading privacy frameworks include risk assessments as one important tool in setting organizations' data protection priorities and safeguarding the most sensitive consumer information.
- *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.
- *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

[1] Washington Privacy Act, SB-5376 (S-1373.7), 66th Leg. (Wash. 2019), http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376-S.pdf.
[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/; Smart Communities: A Conversation with Kelsey Finch, Future of Privacy Forum (Feb. 12, 2019), https://fpf.org/2019/02/12/smart-communities-a-conversation-with-kelsey-finch/.

characterization, and facial recognition. In light of the complexity involved in crafting meaningful regulation of biometric technologies, we recommend that the issue may be better served by a separate, future regulatory effort.

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. Data protection rights and interoperability with existing legal frameworks

FPF has long supported a comprehensive, baseline federal privacy law that fills the gaps between existing sectoral regimes and provides a consistent set of protections for individuals across state lines.[5] Although we are encouraged by recent legislative activity in Congress, the path to a national law remains uncertain.[6] In the absence of a federal law, states that do advance legislation should seek to do so in ways that: (1) provide consumers with comprehensive protections and companies with regulatory clarity; (2) support interoperability with existing state, federal, and international legal frameworks.

For these reasons, we commend the sponsors for addressing a broad set of essential data protection rights, including key elements of the Fair Information Practice Principles (FIPPs). In 1973, the U.S. Department of Health, Education, and Welfare offered the first comprehensive articulation of the FIPPs, expressing principles of transparency, individual control, respect for context, focused collection and responsible use, security, access, and accountability.[7] The FIPPs have since been embodied in United States and international laws, including the EU's General Data Protection Regulation. By codifying a broad set of individual rights – including individuals' rights to access, correct, and delete their personal data; to receive a copy of their personal data; and to restrict or object to the processing of their personal data – the Bill is consistent with these core principles.

As legislators consider amendments to the Bill, we also note that a key element of any state or federal privacy law is that it should avoid conflicting with, and as far as possible promote interoperability with, existing state, federal, and international legal frameworks. The basic principles of the GDPR should provide a reference for policymakers during the legislative process, with an understanding that the U.S. approach to privacy and other constitutional values may diverge in some areas, such as breadth of data subject rights, or implementation of First Amendment values. *See* Attachment 1 (Comparing Privacy Laws: GDPR vs. CCPA).

---

[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 relevant and 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] Long Overdue: Comprehensive Federal Privacy Law, Future of Privacy Forum (2018), https://fpf.org/2018/11/15/fpf-comments-on-a-national-baseline-consumer-privacy-law/; FPF Comments to the U.S. Department of Commerce, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (2018), https://www.ntia.doc.gov/files/ntia/publications/ntia_request_for_comments_future_of_privacy_forum.pdf.

[6] We have noted that a federal baseline privacy law should seek to meet the important goals of clarity and consistency for businesses and consumers while respecting differences in the United States regarding privacy as a fundamental right enshrined in state constitutions. In particular, the Constitution of the State of Washington includes a long-standing fundamental right to privacy that exceeds the protections in the Fourth Amendment. Wash. Const. art. I, § 7.

[7] Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health & Human Services, https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

2. Privacy risk assessments

Risk assessments are a central element of data governance at responsible companies, and a core component of existing privacy regimes in the United States and Europe. For example, in the United States, the Federal Trade Commission (FTC) has required comprehensive privacy oversight programs to include risk assessments in its long history of privacy-related consent decrees.[8] Privacy risk assessments are also the focus of a major ongoing effort by the National Institute of Standards and Technology (NIST),[9] and have been made mandatory for U.S. government agencies.[10]

In the EU, risk assessments are also an important element of the General Data Protection Regulation, which requires assessing risks to determine whether data can be processed based on the legitimate interests of a controller,[11] and more extensive assessments when companies engage in high risk processing.[12] For many US companies engaged in GDPR compliance efforts, a primary focus has been on mapping data flows and conducting assessments to document the purposes of these data flows and the relevant risks and safeguards. This activity benefits consumers, as without risks assessments as a core underlying practice, a company cannot claim to be meaningfully aware of the potential privacy concerns that may be created by its processing of data.

FPF has worked on risk assessments for many years, beginning with a project in 2014 which sought to help provide guidance for big data related risk assessments.[13] In a recent project conducted for the City of Seattle, FPF conducted a privacy risk analysis of the City's Open Data program.[14] While such assessments are only one tool among others in a the context of a comprehensive privacy law, they can be broadly useful and will allow companies to align their compliance efforts with the GDPR as well as the existing FTC guidance for comprehensive privacy programs.

3. 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.[15]

---

[8] *See, e.g.*, Google, Inc., F.T.C. 102 3136 (2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf; Snapchat, Inc.., F.T.C. 132 3078 (2014), https://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf; Uber Technologies, Inc., F.T.C. 152 3054 (2018), https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_decision_and_order.pdf; ASUSTeK Computer, Inc., F.T.C.142 3156, https://www.ftc.gov/system/files/documents/cases/160222asusagree.pdf. *See also, generally*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014).
[9] Privacy Risk Assessments: A Prerequisite to Privacy Risk Management, National Institute of Standards and Technology (2017), https://www.nist.gov/sites/default/files/documents/2017/06/05/privengworkshop_preso.pdf.
[10] *See* Revision of OMB Circular A-130, "Managing Information as a Strategic Resource," FR Doc. 2016-17872 (July 28, 2016), https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.
[11] Regulation (EU) 2016/679 General Data Protection Regulation, 2016 O.J. (L. 119) 1, Recital 47, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.
[12] *Id.* at Article 35.
[13] Jules Polonetsky et al., *Benefit-Risk Analysis for Big Data Projects*, Future of Privacy Forum (Sept. 2014), https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf.
[14] *See* Joseph Jerome, *Big Data: A Benefit and Risk Analysis*, Future of Privacy Forum (Sept. 11, 2014), https://fpf.org/2014/09/11/big-data-a-benefit-and-risk-analysis/.
[15] Digital Data Flows Masterclass, Future of Privacy Forum, https://fpf.org/classes-archives/.

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").[16] 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.[17] We hope our resources in this field can be of assistance to the Committee and are available to engage further.

4. Facial recognition

We commend the sponsors of the Bill for recognizing the privacy implications of facial recognition as a uniquely sensitive data processing activity. In recent years, FPF has published resources (see below, Additional Resources) on the distinctions between related technologies, including facial detection, facial characterization, and facial recognition, and how companies may use these technologies while mitigating or avoiding privacy risks. We note, in light of the complexity involved in crafting meaningful regulation of biometric technologies, that the issue would likely be better served by a separate, future regulatory effort. FPF would be pleased to engage further with the Committee on this important issue.

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):

- *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.
- *Facial Recognition***.** In September, 2018, FPF published the infographic *Understanding Facial Detection, Characterization, and Recognition Technologies*, along with *Privacy Principles for Facial Recognition Technology in Consumer Applications*. These resources are intended to help policymakers better understand and evaluate the growing use of consumer-facing technologies used for facial detection, characterization, and recognition.[18]

---

[16] 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.

[17] *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), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2827&context=lawreview.

[18] For more on these resources, visit: https://fpf.org/2018/09/20/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/.

- *Genetic Data*. In 2018, FPF convened a working group of leading direct-to-consumer (DTC) genetics companies, to develop Privacy Principles for Genetic Data. These Principles provide a privacy policy framework for the collection, protection, sharing, and use of genetic data.[19]
- *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.[20]

We hope these comments and attached 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

Stacey Gray
Policy Counsel
Future of Privacy Forum
1400 Eye St. NW Ste 510,
Washington, DC 20005

See Attachment 1: "Comparing Privacy Laws: GDPR vs. CCPA"
also available at www.fpf.org

[19] Privacy Best Practices for Consumer Genetic Testing Services, Future of Privacy Forum (Jul. 31, 2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.
[20] Digital Data Flows Masterclass, Future of Privacy Forum, https://fpf.org/classes/.