FUTURE OF PRIVACY FORUM

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

September 30, 2020

Senator Reuven Carlyle
36th District, Seattle
720 N 35th St. #209
Seattle, WA 98103

Dear Senator Carlyle,

The Future of Privacy Forum (FPF) writes to share our thoughts on the current draft Washington Privacy Act 2021.[1] FPF is a non-profit organization advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally.[2] Our office in Seattle, WA is the center for our Smart Communities project, an effort that brings together local privacy leaders implementing smart city projects at municipalities around the country to help them develop robust data protection frameworks.

In the midst of a global pandemic and in the absence of a baseline federal privacy law, we commend the legislature's continued commitment to privacy and your ongoing leadership role. We have written previously, and reiterate here, that the protections in the Washington Privacy Act ('WPA' or 'the Act') go beyond the protections in the California Consumer Privacy Act ('CCPA') and provide a comparatively stronger model for data protection in the United States.[3] The Act's overall structure closely aligns with contemporary, global data protection approaches,[4] and is a good compromise that achieves the right balance of protecting personal data while supporting commerce and research.

However, we have observed deep polarization in legislative debates in recent years, both in Washington and elsewhere. Given the importance of the issues involved in advancing data protection, it's no surprise that stakeholders are passionate about this discussion. But given the challenges our country faces, the need to reach consensus is more important than ever, and we view meaningful legal privacy protections as both necessary and achievable.

Below, we identify a number of relevant points of debate between stakeholders, along with practical suggestions for how they might be addressed in the context of the WPA. We note that there are a range of views on some of these issues, and our goal is to provide practical options for paths forward. These include: (1) exemptions for scientific research; (2) enforcement by the Attorney General; and (3) the limitations of opt-in and opt-out regimes. We are also (4) supportive of the strong collection and use safeguards that Parts 2 and 3 of the Act would place on data collected for purposes of addressing the COVID-19 pandemic.

[1] Draft circulated Aug. 5, 2020, http://sdc.wastateleg.org/carlyle/wp-content/uploads/sites/30/2020/09/WPA-2021-DRAFT-Carlyle.pdf
[2] The views herein do not necessarily reflect the views of our supporters or Advisory Board.
[3] *FPF Comments on WPA* (Dec. 13, 2019), https://fpf.org/wp-content/uploads/2020/09/FPF-Comments-on-v1-Washington-Privacy-Act-Dec.-13-2019-1.pdf.
[4] *A New U.S. Model for Privacy?* (Feb. 12, 2020), https://fpf.org/2020/02/12/a-new-model-for-privacy-in-a-new-era-evaluating-the-washington-privacy-act/.

(1) Exemptions and Scientific Research (Section 110)

WPA Section 110 provides exemptions from the Act's obligations for organizations engaged in scientific research and other activities, such as fraud detection, internal operations, and product improvement. Privacy advocates have raised concerns over the scope of these exemptions, on the grounds that if they are too broad or untethered, they can easily become loopholes. Data processors and controllers worry that narrow exemptions would prevent the necessary flexibility for engaging in legitimate, routine, or low-risk operations that would otherwise be unduly hindered by requirements to obtain permission or operationalize consumer requests. Below we offer practical recommendations for Section 110.

With regard to research, the Act exempts controllers and processors from all obligations to the extent that they are engaged in:

> **"public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws as long as such processing is disclosed to the individual . . ." (Section 110(h))**

Data-driven research can lead to socially beneficial, generalizable scientific knowledge, and such research can conflict with privacy bills' deletion and consent requirements. For example, consent may be impossible or impractical when dealing with large, not readily identifiable datasets, and deletion requests can sometimes lead to biased or unrepresentative samples ("consent bias"), insufficient sample sizes, delays, or other costs to researchers.

However, an exemption for research with no additional limits on data processing is likely too broad. Instead, we recommend an approach that would create oversight for organizations that engage in such research by requiring it to be approved, monitored, and governed by an Institutional Review Board (IRB) or similar oversight entity.

A more tailored research exemption might be:

> **"(h) engage in scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an Institutional Review Board (IRB), human subjects research ethics review board, or similar independent oversight entity that determines that:**
> **(i) the research is likely to provide substantial benefits that do not exclusively accrue to the controller;**
> **(ii) the expected benefits of the research outweigh the privacy risks; and**
> **(iii) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification."**

Similarly, other exemptions in Section 110, such as exemptions that facilitate processing for internal operations or anti-fraud operations, could be more narrowly tailored in scope or application. For example, certain exemptions could be applied only to WPA requirements for consent, correction, or deletion (Sections 103-105) while preserving requirements that organizations maintain reasonable security practices, minimize data collection when appropriate,

apply purpose limitation principles (Section 107), or conduct Data Protection Assessments (Section 109).

Additional Resources:

- FPF, *Beyond IRBs: Designing Ethical Review Processes for Big Data Research* (Conference Proceedings) (Dec. 10, 2015), https://fpf.org/wp-content/uploads/2017/01/Beyond-IRBs-Conference-Proceedings_12-20-16.pdf
- Mike Hintze, *Science and Privacy: Data Protection Laws and Their Impact on Research* (June 19, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3402702
- Dr. Sara Jordan, *Designing an Artificial Intelligence Research Review Committee* (Sept 2019), https://fpf.org/wp-content/uploads/2019/10/DesigningAIResearchReviewCommittee.pdf
- FPF Webinar, *Commercial Research* (Dec. 6, 2019), https://fpf.org/legislative-resources/#topic2

(2) Enforcement by the Attorney General (Section 112)

Enforcement is critical to a privacy law's success. Effective, predictable enforcement establishes meaningful protections for individuals and gives organizations clarity about their obligations. Currently, the Act provides for enforcement by the Washington State Attorney General, with a thirty day right to cure, and other internal accountability mechanisms, including mandated Data Protection Assessments (DPAs) that can be accessed upon request by the Attorney General.

Under the GDPR, individuals have the right to file complaints with their regulator (Data Protection Authorities or DPAs), to challenge violations in court, and in some cases to be represented by non-profit organizations (NGOs). Similarly, a future national framework in the United States might incorporate US-specific methods for individual redress in order to meet at least some requirements for achieving EU adequacy.[5] Notably, however, the legal culture and procedural norms for large, contingency-based class action lawsuits are not a current feature of EU law.[6] Furthermore, by the time the GDPR took effect in 2018, the EU had a longstanding history of privacy and data protection legal compliance and guidance materials from regulators, dating back to the 1995 Data Protection Directive.[7]

Recent legislative debates have featured privacy advocates promoting a private right of action as an enforcement mechanism and companies opposing private rights of action while supporting a single enforcement entity - typically an attorney general or an independent consumer protection regulator. Washington lawmakers may reasonably conclude that the benefits of private litigation (strength and individual empowerment) are outweighed by its potential risks (impact on small businesses and legal uncertainty). We suggest that no matter where lawmakers fall on this question, there are a range of enforcement options that can increase or decrease accountability, enforcement, legal clarity, and options for consumers.

---

[5] Information Commissioner's Office, *Assessing Adequacy: International Data Transfers*, https://ico.org.uk/media/for-organisations/documents/1529/assessing_adequacy_international_data_transfers.pdf.
[6] Michael Thaidigsmann, *EU Plans to Allow Class Action Suits – Under Certain Terms* (Apr. 11, 2019), https://inhouse-legal.eu/corporate-ma/collective-redress/.
[7] Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf.

Key options for strengthening Attorney General enforcement:

- **Right to cure (Section 112).** The WPA contains a thirty-day right to cure period, which allows the AG to vindicate violations efficiently and quickly and companies to come into compliance quickly without incurring financial penalties. It also allows the AG to bring large numbers of businesses into compliance with a new law, while requiring relatively little additional efforts from the enforcement entity. For example, the Attorney General of California recently testified that large numbers of enforcement letters sent in July 2020 have led to "substantial compliance" with the CCPA.[8]
- **Internal appeals (Section 105).** The WPA requires covered entities to provide a conspicuous and easy to use internal appeals process for consumers to appeal a refusal to take action on a request to exercise rights. An internal appeals process can provide for a non-judicial resolution of claims, in particular for outcomes that are the result of mistakes or oversights, reserving the investigations and enforcement resources of the Attorney General for more serious or widespread violations. For consumers, using internal appeals processes to handle disputes can lead to quicker and less costly remedial action. In addition to providing consumers with a non-judicial resolution for their claim, internal appeals can also reduce legal uncertainty for businesses.
- **Increasing funding for staff, expenses, and an office of technology research.** The legislature should fully fund the office of the Attorney General, including for legal and technical staff to investigate and address violations, engage in consumer education, and promulgate guidance. Similarly, Washington lawmakers may choose to follow the model of the Federal Trade Commission, which has a dedicated Office of Technology Research and Investigation (OTech) to conduct independent studies, evaluate emerging technologies, assist investigators and attorneys, and provide technical expertise and training. Similar expertise in Washington would allow the AG to bring more targeted and effective enforcement actions.
- **Complaint resolution.** The Act could bolster the existing informal complaint resolution services offered by the Consumer Protection Division of the office of the Attorney General. This process includes notifying businesses of complaints and facilitating communication between the consumer and the business to assist in resolving the complaint.[9] Such services could be strengthened through funding and staff, or formalized to include additional requirements, for example that the office address and resolve complaints (a method of individual redress), or publicize aggregate statistics about complaints filed.
- **Tiered effective dates.** A tiered structure for enforcement provisions could help ensure increasingly strong enforcement over time while giving companies time to adapt and build compliance structures for a new law. For example, any additional funding, rulemaking, or guidance authority for the Attorney General should begin immediately, rather than waiting until the Act's substantive requirements come into effect, to give the office time to build expertise and draft guidance. Enforcement through injunctive relief could begin at an early stage, to provide further clarity, and civil penalty authority could

[8] Revisiting the Need for Data Privacy Legislation: Hearing Before the S. Comm. on Commerce, Science, and Transportation (Sept. 23, 2020), https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation.
[9] *Consumer Protection*, Washington State Office of the Attorney General, https://www.atg.wa.gov/consumer-protection.

come into effect at a later stage. A staged rollout could help alleviate concerns over legal clarity and the novelty of new provisions for businesses, while ensuring stronger long-term enforcement.

(3) Emerging technology and the limits of "opt in" vs. "opt out"

The WPA requires that entities obtain "freely given, specific, informed, and unambiguous" consent (Section 101(5)) prior to the collection of sensitive data, and requires organizations to provide an opportunity for consumers to "opt out" of targeted advertising, sale, or profiling in furtherance of decisions that produce legal or similarly significant effects (Section 103(5)). These provisions build upon and go farther than the CCPA's requirement that individuals be able to opt out of "sale."

We observe that there are limitations to both "opt-in" models and "opt-out" models, especially for emerging technologies. Opt-out options can be unwieldy, hard to find, and rarely used by consumers, particularly for organizations processing data that do not have a direct business-to-consumer relationship. On the other hand, opt-in models can lead to notice fatigue, consent bias, impracticality, or be unworkable for consumers who are unable to adequately weigh the risks and benefits to complex downstream data practices. Finally, both models assume the existence of a user interface through which a user exercises a choice, which is not always possible. For example, connected and automated vehicles typically collect large amounts of data, including images and video data, from external sensors. Obtaining consent from pedestrians or other drivers may be impossible or undesirable to rely on; instead, other privacy safeguards (such as de-identification, use limitations, and retention limits) are needed.

Given these challenges, the WPA achieves a balanced compromise by taking a risk-based, and globally interoperable approach to data collection that incorporates Data Protection Assessments (DPAs). This goes significantly beyond the CCPA and other "notice and choice" models, shifting more of the burden of compliance from individuals to the organizations processing data. It also aligns more closely with the GDPR, which requires Data Protection Impact Assessments for high-risk data processing, and explicit consent to process "special categories of data."[10]

Provisions of the WPA that create protections for individuals beyond opt-in and opt-out models, or might do so in the future, include:

- **Data Minimization.** An essential part of the Fair Information Practice Principles (FIPPs), and required by the GDPR (Art. 5), "data minimization" is the requirement that covered entities only collect and retain personal information that is directly relevant, adequate, and necessary to accomplish specific lawful purposes. **(Section 107)**
- **Purpose Limitation.** Another principle of lawful data processing, "purpose limitation" requires that data collected for a specific purpose not be further processed in a manner that is incompatible with those purposes **(Section 107)**. We recommend that WPA follow the lead of the GDPR and clarify that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in

[10] Regulation (EU) 206/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data dn on the free movement of such data (hereinafter "GDPR"), art. 9.

accordance with [pseudonymization and other safeguards], not be considered to be incompatible with the initial purposes."[11]

- **Balancing Tests.** In addition to consent, some global regimes rely on legal balancing tests that weigh the legitimate uses of data against the impact on individual privacy and other rights. Often, such balancing tests can rely on the outcome of a Data Protection Assessment (DPA) **(Section 109)** to limit the uses of data collected without consent or ability to opt-out. For example, the GDPR allows businesses to rely on a "legitimate interest" to process data if not outweighed by the interests or fundamental rights and freedoms of the individual.[12]
- **Alignment with Other Legal Regimes.** Lawmakers should look to other emerging proposals in the United States to promote interoperability between legal privacy and data protection obligations. For example, aligning the definition of "sale" in the WPA with the definition of "sale" in the CCPA would allow companies to streamline compliance with a single opt-out mechanism across borders.

(4) Public health provisions for COVID-19 (Parts 2 and 3 of WPA)

We strongly support the public health provisions in Part 2 of the Act as currently drafted, and commend legislators for soliciting broad public input on these issues.[13] In upcoming years, the use of data for contact tracing and exposure notification is likely to continue to be a core part of public health efforts. Preliminary evidence from other global efforts suggests that digital contact tracing apps can have a positive impact on reducing the rate of COVID-19 infection, if used to supplement robust testing and other measures. For example, even at adoption rates far below 60%,[14] preliminary evidence regarding the SwissCovid app in Switzerland indicates that decentralized exposure notification tools based on the Google-Apple API can increase actions taken by exposed contacts to seek treatment.[15]

Meanwhile, adoption of contact tracing apps in the U.S. has been notably low compared to abroad,[16] due to issues of trust. Adoption of contact tracing and exposure notification technologies, such as the CommonCircle app,[17] requires that individuals trust that data will not be

[11] GDPR arts. 5, 89(1).
[12] *See* Gabriela Zanfir-Fortuna & Nymity, *Deciphering Legitimate Interests: A Report Based on More Than 40 Cases from Practice* (Mar. 14, 2019), https://www.lexology.com/library/detail.aspx?g=ba9dd603-2f73-4e42-a015-9fd130b2b724; Information Commissioner's Office, *Legitimate Interests*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.
[13] Pollyanna Sanderson, *FPF Presents Expert Analysis to Washington State Lawmakers as Multiple States Weigh COVID-19 Privacy and Contact Tracing Legislation* (Aug. 26, 2020), https://fpf.org/2020/08/26/state-trends-in-covid-19-privacy-and-contact-tracing-legislation/
[14] Patrick Howell O'Neill, *No, coronavirus apps don't need 60% adoption to be effective,* MIT Tech Review, (June 5, 2020), https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.
[15] Marcel Salathe et al., *Early Evidence of Effectiveness of Digital Contact Tracing for SARS-CoV-2 in Switzerland*, https://github.com/digitalepidemiologylab/swisscovid_efficacy/blob/master/SwissCovid_efficacy_MS.pdf.
[16] For example, Germany, Ireland, and Switzerland have adoption rates between 17% and 38% for their decentralized Bluetooth-based apps. In contrast, North Dakota, Utah, and Rhode Island's centralized GPS location-based apps have seen adoption rates of between 1% and 4%. *See* Charlotte Jee, *Is a successful contact tracing app possible? These countries think so*, MIT Tech Review (Aug. 10, 2020) https://www.technologyreview.com/2020/08/10/1006174/covid-contract-tracing-app-germany-ireland-success/; *See also* Tyler Sonnemaker, *Utah spent nearly $3 million on a contact tracing app that less than 2% of the state's population has downloaded*, Business Insider (May 2, 2020), https://www.businessinsider.com/utahs-275-million-contact-tracing-app-few-downloads-report-2020-5 .
[17] *CommonCircle*, https://commoncircle.us/.

mis-handled, retained indefinitely, or re-purposed for non-public health purposes by the government or private companies. For this reason, it is essential to pass strong privacy laws that balance strong, clear protections for individuals with the flexibility needed to use data to measure health outcomes and address the pandemic.

As discussed during FPF's presentation on government uses of data and contact tracing technologies at a public work session in August,[18] the following WPA provisions align with guidance from FPF and other leading experts:

- Prohibition on access to public health data for law enforcement or immigration;
- Retention limitations;
- Voluntariness of app usage;
- Confidentiality;
- Security;
- Transparency;
- Processing opt-outs, as well as access, correction, and deletion rights for individuals to promote individual empowerment and trust.

Additional Resources for COVID-19 and Privacy:

- FPF *Privacy and Pandemics* Series, https://fpf.org/privacy-and-pandemics/
- Wiki of COVID-19 Resources, https://fpf.org/covid-19-resources/
- FPF & BrightHive, *Digital Contact Tracing: A Playbook for Responsible Data Use* (August 14, 2020), https://law.mit.edu/pub/digitalcontacttracingaplaybookforresponsibledatause/release/1
- Infographic, *Understanding the World of Geolocation Data* (May 22, 2020), https://fpf.org/2020/05/22/understanding-the-world-of-geolocation-data/
- Gabriela Zanfir-Fortuna, *European Union's Data-Based Policy Against the Pandemic, Explained* (April 30, 2020), https://fpf.org/2020/04/30/european-unions-data-based-policy-against-the-pandemic-explained/
- FPF, *Reopening Schools Issue Brief: Location Tracking & COVID-19* (August 13, 2020) https://studentprivacycompass.org/reopening-4/

We hope these comments 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
Senior Counsel
Future of Privacy Forum
PO Box 14051
Seattle, WA 98144

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

[18] Pollyanna Sanderson, FPF Presents Expert Analysis to Washington State Lawmakers as Multiple States Weigh COVID-19 Privacy and Contact Tracing Legislation (Aug. 26, 2020), https://fpf.org/2020/08/26/state-trends-in-covid-19-privacy-and-contact-tracing-legislation/.