Washington Consumer Data Privacy Legislative Proposals – Technology Law and Public Policy Clinic Recommendations

I. Introduction:

The Washington State Legislature has recognized the importance of comprehensive consumer data privacy legislation since 2019, when the original Washington Privacy Act (“WPA”) (SB 5062) was proposed in the Senate but failed to get a floor vote in the House.1 Following this effort, the House introduced the People’s Privacy Act (HB 1433) in 2021 as a “pro-consumer” alternative to SB 5062.2 Finally, an effort to blend elements of both proposals was introduced during this past session, in an effort to pass the Washington Foundational Data Privacy Act (HB 1850).3

Despite Washington’s failure to pass a comprehensive data privacy bill, other states have used the WPA as a model for enacting their own data privacy legislation. Meanwhile, the Washington legislative process continues debate regarding various provisions of a potential data privacy act. The announcement that Senator Carlyle, sponsor of the original WPA, is exiting the Senate will no doubt change the landscape of legislative proposals. Amidst the backdrop of a growing national conversation surrounding consumer data privacy, and a wave of other states passing legislation, the future of the Washington state policy debate is uncertain.

This white paper will consider specific provisions which have made up areas for contention in the Washington legislative process: the opt-in versus opt-out models of consumer consent, the private right of action, and the privacy commission introduced in HB 1850. The paper will conclude by making recommendations regarding a future Washington state consumer data privacy bill. As an appendix, this paper also provides aggregated character studies of Washingtonians to illustrate the ways in which consumers might navigate resources and remedies provided by a state data privacy act.

II. Provisions of Data Privacy Regulation

a. Opt-in/out

Many people who engage online are familiar with “cookies,” attaching at least a vague association of the term with how websites collect information on individual visitors. All websites (including phone apps) collect cookies: some cookies are necessary to operate the site or app, while others collect unnecessary data that is often shared with third parties. Often, this data is sold or shared with the government or law enforcement. There is a common misconception that the reason we receive targeted advertisements is because our phones are “listening” to our conversations (we mention to a friend that we want to buy a new TV, and like magic our

browsers are filled with pop-up ads for TVs). While this is sometimes true (phones can listen for Siri commands, text-to-talk, or other usability features), most of the time we have already told websites what to advertise to us. We have allowed websites to track our data, creating interest profiles based off our web browsing and information shared by our friends or close circles. This exchange of information among likeminded groups helps algorithms build profiles so that advertisers can target potential customers.

In the U.S., internet and telecommunications users most commonly encounter an “opt-out” model of data collection and use. This model allows organizations to collect data by default but provides users the option to opt out of the sale of that data to third parties. States that have passed consumer data privacy legislation have all included opt-out provisions, with an exception among some states requiring an opt-in default for users sixteen years of age and younger. This contrasts with the primary European consent model, codified in the European Union’s General Data Protection Regulation (“GDPR”). As more states adopt consumer data privacy legislation, and federal legislators consider a future federal data privacy act, there is debate whether U.S. data privacy laws should include an opt-in consent requirement.

**Opt-In Consent**: Opt-in consent means that an individual user manually provides consent to the website or telecommunication service (i.e. email marketing) before that provider can collect, store, or use (including sell) the data exposed by the user. Typically, the individual gives consent by checking boxes or “accepting” terms of data collection before accessing a website. For telecommunication (text messages or electronic mail), opt-in consent typically requires the individual to check “yes” or “no” to receiving further communications from the organization.

The most robust model of a strictly opt-in framework can be found in the GDPR, which sets a broad standard of requiring consent that is “freely given, specific, informed and unambiguous,” going so far as explicitly prohibiting consent based on “pre-checked boxes.” While this is the standard for internet users in EU member states, U.S. states have been reluctant to implement such broad restrictions. However, one example of U.S. companies modeling an opt-in framework can be found in email marketing. Some companies elect to adopt opt-in marketing standards for email communications in the hopes of enhancing transparency and consistency for customers worldwide.

**Consent Framework Debate in Washington**: The WPA includes an opt-out consent model, stipulating that the consumer has a right concerning processing of personal data for purposes of targeted advertising, sale of personal data or “profiling in furtherance of decisions that produce

---

4 Dana Rezazadegan, Is your phone really listening to your conversations? Well, turns out it doesn’t have to, The Conversation (June 20, 2021), https://theconversation.com/is-your-phone-really-listening-to-your-conversations-well-turns-out-it-doesnt-have-to-162172.

5 Id.

6 California Consumer Privacy Act (CCPA; effective Jan. 1, 2020), Colorado Privacy Act (SB 190; effective July 1, 2023), Virginia Consumer Data Protection Act (SB 1392; effective Jan. 1, 2023), Utah Consumer Privacy Act (SB 227; effective Dec. 31, 2023).

7 California and Colorado require opt-in default for users 16 and under, while Virginia and Utah lower that age to users 13 or younger.

8 In the U.S. the CAN-SPAM Act and the TCPA provide limitations for companies engaging in email and telephone marketing.
legal effects concerning a consumer or similarly significant effects concerning a consumer.”

It requires data controllers to obtain opt-in consent only for sensitive data. Advocating in favor of opt-out consent, Senator Carlyle has testified in House committee meetings that requiring opt-in consent for every online interaction would overwhelm consumers with “notice fatigue.”

In committee meetings, critics of the opt-out model claimed that a right to opt out is not the equivalent of informed consent. In compiled testimony, opponents testified that the approach “has threatened the personal safety of the lives of many survivors of domestic violence and abuse.” Additionally, opponents testified that the opt-out framework does not “adequately protect the privacy of the immigrant and refugee communities,” many of whom “have a limited understanding of technology, as well as limited English language skills,” and thus would likely have difficulty understanding how to utilize opt-out consent.

Alternatively, HB 1433, the People’s Privacy Act, would have implemented an opt-in consent requirement prior to use or disclosure of personal information. The bill regarded opt-in consent as essential to protecting privacy, noting in the language of the bill that without it, individuals would “face an unsurmountable challenge of identifying and engaging with each and every entity they encounter.” By contrast, the most recent House bill—HB 1850, the Foundational Data Privacy Act—provided for a hybrid but generally opt-out consent model regarding targeted advertising, sharing of personal data (which does not apply to sharing with affiliates), and profiling. HB 1850 required “controllers must provide an effective mechanism for a consumer to revoke consent.” The Foundational Data Privacy Act would have created an exception for the collection of sensitive data, requiring opt-in consent.

Industry parties advocate for general opt-out frameworks, while privacy and technology justice advocates favor a strict opt-in framework. A proponent of the original HB 1433, the ACLU of Washington criticized HB 1850’s opt-out framework, advocating instead for the adoption of the GDPR definition of “consent.” Advocates for opt-in consent argue that even seemingly innocuous data collected by controllers and processors can be used “to infer ‘sensitive’ information such as racial or ethnic origin, mental or physical health conditions, sexual orientation, or citizenship or immigration status.”

The different positions represent different ideological approaches to data privacy and priorities of data regulation. Proponents of SB 5062 emphasized user experience and viability of data controllers and processors to comply with consent requirements. However, proponents of the opt-in framework emphasize equity concerns, warning that the privacy implications of opt-out consent will be felt most acutely by consumers

9 SB 5062.
11 Id.
12 Id. Testifying opponents included the Tech Equity Coalition, Council on American-Islamic Relations Washington, ACLU of Washington, and La Resistencia.
13 Id. p. 19.
15 Id.
in marginalized groups. Additionally, they warn that consumers who are not English-speaking may be particularly vulnerable to illegal data harvesting.\(^\text{16}\)

\(\text{b. Private right of action}\)

\textbf{Value of a private right of action:} One of the most contentious issues in Washington’s efforts to pass a consumer privacy bill has been determining the appropriate mechanism for individuals to enforce their rights. Whether or not to include a private right of action has been a primary component of that debate. A private right of action allows individuals to enforce their rights by suing an opposing party\(^\text{17}\). A private right of action has inherent benefits. First, the right of an aggrieved party to file suit is a fundamental feature of the U.S. justice system. Additionally, a private right of action helps hold wrongdoers accountable by creating an avenue for them to be sued by those impacted by their actions. Also, a private right of action helps marginalized communities, which are often overlooked by traditional government enforcement regimes. Marginalized individuals historically have not been able to rely on the government to protect them\(^\text{18}\), and a private right of action empowers these individuals to directly enforce their rights.

\textbf{Benefit of private right of action compared to alternatives:} Enforcement by a consumer data privacy commission and enforcement by the Attorney General (“AG”) are two alternative enforcement mechanisms that have been proposed.

(a) \textbf{Commission Enforcement:} A consumer data privacy commission would be a newly created expert body within the government that is empowered to initiate investigations of misconduct and impose penalties on violators. Leveraging a commission with the background, expertise, and resources to enforce a bill would be helpful for many aggrieved individuals. However, there would be some individuals who do not agree with the resolution reached by the commission. Rather than forcing these individuals to abide by the commission’s outcome with no other recourse, a private right of action would offer these individuals a path forward to seek justice.

(b) \textbf{Attorney General Enforcement:} The AG’s office is accustomed to investigating entities that have aggrieved individuals and adding consumer data privacy to the AG’s docket has been suggested. However, the AG’s office has said it cannot enforce a data privacy bill by itself due to resource constraints\(^\text{19}\). Additionally, one cannot know who the AG will be and to what extent data privacy enforcement would be a priority for that AG at any particular time. A private right of action protects against these drawbacks by giving individuals an option to proceed in the event they are unsatisfied with the outcome reached by the AG.

\(^\text{16}\) HB 1850 Feedback, ACLU of Washington; Committee Report on Washington Privacy Act.


\(^\text{19}\) Jennifer Lee’s discussion with our clinic on 11/3/21.
Concerns of a private right of action: Opponents of including a private right of action believe doing so would result in frivolous lawsuits being filed, benefiting plaintiff’s lawyers but overcrowding and burdening the court system. However, limitations can be placed on a private right of action to reduce the number of lawsuits filed. For example, the California Consumer Privacy Act (“CCPA”) includes a limited private right of action where individuals can only sue a business under CCPA if there is a data breach, and even then, only in limited circumstances\(^\text{20}\). Only the California AG can file suit against businesses for all other CCPA violations\(^\text{21}\). Roughly 125 lawsuits were filed under the CCPA in 2021\(^\text{22}\). As Washington’s population is about 20% of California’s\(^\text{23}\), Washington would likely not anticipate a burdensome amount of lawsuits being filed in the event it passes consumer data privacy legislation with a limited private right of action.

Other locales:
GDPR: GDPR does not include a private right of action provision. GDPR instead calls for supervisory authority, requiring that “[e]ach Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation.\(^\text{24}\)” GDPR provides individuals who believe their rights have been infringed with the right to lodge a complaint with a supervisory authority\(^\text{25}\).

Other states: Four states have enacted consumer data privacy laws in the US: California, Virginia, Colorado, and Utah.

(a) California: For most violations of the CCPA, only the California AG can file a suit. However, the CCPA includes a limited private right of action where a California resident can file suit where his or her nonencrypted and nonredacted personal information was stolen in a data breach, due to the business’s failure to maintain reasonable security procedures and practices to protect it.\(^\text{26}\) The stolen personal information must include (1) the individual’s first name (or first initial) and last name; and (2) one of the following: social security number; unique identification number issued on a government document commonly used to identify a person's identity (such as driver’s license number); financial account number, credit card number, or debit card number that if combined with any required security code, access code, or password would allow someone access to the individual’s account; medical or health insurance information; or unique biometric data used to identify a person's identity, such as a fingerprint, retina, or iris image. If these criteria are met, an individual can sue for actual monetary damages or for statutory

\(^{20}\) California Consumer Privacy Act (CCPA), State of California Department of Justice, https://oag.ca.gov/privacy/ccpa.

\(^{21}\) Id.


\(^{24}\) See GDPR Art 51.1. The full GDPR is available at https://gdpr-info.eu/.

\(^{25}\) GDPR Art 77.1.

\(^{26}\) CCPA: A consumer bringing an action… shall notify the Attorney General within 30 days that the action has been filed. The Attorney General… within 30 days… [shall] notify the consumer [of intent] to prosecute an action against the violation.” 1798.150(2)-(3)(A). CPRA Commission: 5-member commission for “full administrative power, authority, and jurisdiction to implement and enforce” the CCPA.
damages of up to $750 per incident. Individuals wishing to sue for statutory damages must first provide the business with a 30-day right to cure period. Additionally, the California Privacy Rights Act, which takes effect in 2023, amends and expands the CCPA by creating a new California Privacy Protection Agency to share oversight and enforcement with the AG.

(b) **Virginia:** The Consumer Data Protection Act does not include a private right of action; rather it vests enforcement authority solely in the AG’s office.  
(c) **Colorado:** The Colorado Privacy Act does not include a private right of action; rather, it vests enforcement authority in the AG and District Attorney’s offices.  
(d) **Utah:** The Utah Consumer Privacy Act does not include a private right of action; rather, it vests enforcement authority solely in the AG’s office.

**Washington Private Right of Action Debate:** In Washington, the Senate’s WPA does not include a private right of action. Rather, it instead calls for enforcement solely by the AG’s office, under the consumer protection act. In the House, the original version of the Foundational Data Privacy Act included three layers of enforcement: (1) enforcement by the Consumer Data Privacy Commission; (2) enforcement by the AG; and (3) a private right of action. The private right of action allowed parties to win an injunction and actual damages. Before filing a lawsuit, the bill called for a party to provide thirty days’ notice to the defendant and to the Commission, and to give the defendant the thirty-day period to resolve the issue.

However, by the end of the session, in an effort led by the Governor’s office to merge the House and Senate bills, HB 1850 was ultimately stripped of its private right of action and now includes only enforcement via the Commission. If the Commission finds that a violation occurred and that an individual suffered actual damages, the individual may then bring suit under the Consumer Protection Act, with available remedies being an injunction, actual damages, and recovery of attorneys’ fees.

---

35 Id.

36 Id. section 20(2)(a-b).  
38 Id.
Reducing the conversation surrounding enforcement to a singular private right of action assumes private litigation is sufficient to protect the rights of citizens against an abundance of corporate legal resources. The Commission enforcement structure proposed by HB 1850 offers the potential for equitable access to the enforcement of consumer data privacy rights without requiring individuals to retain private counsel. In this way, the Commission can assist Washingtonians in navigating a complex legal system rather than further perpetuating inequality.

c. **Washington Consumer Data Privacy Commission**

Additionally, HB 1850 would create the Washington Consumer Data Privacy Commission to “balance the goals of strengthening protections for consumers’ fundamental right to privacy while giving attention to the impact on controllers and processors.” This proposed Commission provides a unique opportunity for Washington to invest in the infrastructure necessary to support equitable consumer privacy protection and to serve as a national model for future legislation. As an independent expert body, the Washington Consumer Data Privacy Commission would serve an important role as a buffer separating consumer data privacy rights from the influence of individual legislators or interest groups.

**Commission Structure:** Under HB 1850, the Washington Consumer Data Privacy Commission would be composed of three governor-appointed individuals with “qualifications, experience, and skills . . . in the areas of privacy and technology.” The Commission would also appoint an executive director, who will “have such powers as the commission may prescribe and delegate” to implement and enforce the privacy rights of Washingtonians efficiently and effectively. The Commission may additionally employ technical, administrative, and other staff as necessary to support the commission’s prescribed duties and powers. The Commission would receive administrative support from the Washington Transportation and Utilities Commission; however, the Washington Consumer Data Privacy Commission would remain independent in exercising its powers, functions, and duties.

**Duties, Powers, and Rulemaking Authority:** The Commission would be vested with rulemaking authority under the Administrative Procedure Act (RCW 34.05) to “adopt, amend, and rescind suitable rules . . . to carry out the purposes and provisions of the commission”. The Commission would also serve an important role as an expert body, providing technical assistance to the legislature with regards to privacy-related legislation as well as developing guidance to inform Washingtonians of their rights and to guide controllers and processors in complying with their obligations and duties under the law. Information provided by controllers and processors of consumer data would be publicly accessible on the Commission’s web page. Additionally, the Commission would establish and collect an annual registration fee equal to one-tenth of one

39 HB 1850 § 2(1)(k).
40 HB 1850 § 1(3)(a).
41 HB 1850 § 1(5).
42 HB 1850 § 1(6).
43 HB 1850 § 2(1)(k)(1).
44 HB 1850 § 2(1)(b).
45 HB 1850 § 2(1)(e).
46 HB 1850 § (2)(d).
47 HB 1850 § 2(1)(k)(1).
percent of intrastate gross operating revenue from each controller or processor that operates within the state and earns at least $20,000,000 annually in gross operating revenue. These annual fees would be deposited into a newly-created Consumer Privacy Account and be used solely to fund the Commission’s operating expenses.

**Commission Enforcement:** Additionally, the Commission would be vested with the authority to review and investigate alleged violations of Washingtonians’ privacy rights, initiated on its own or by consumer complaint. To facilitate these investigations, the Commission would have the power to “subpoena witnesses and compel attendance, take the testimony of any person under oath, [and] subpoena the production of any books, papers, records, or other items material to . . . its power to audit a controller or processor’s compliance.” The Commission would have discretion to decide whether to investigate a complaint or provide additional time to cure the alleged violation, taking into consideration the controller or processor’s lack of intent to violate the law and any voluntary efforts undertaken to cure the alleged violation prior to receiving a complaint. Alternatively, the Commission may refer a received complaint to the AG for civil enforcement.

The Commission must provide a controller or processor with at least thirty days’ notice of the alleged violation and a summary of the supporting evidence, as well as inform them of their right to be present and represented by counsel at any proceeding held to determine whether there is reason to believe a violation occurred. If the Commission determines there is reason to believe a violation occurred, the Commission must issue a warning letter to the controller or processor identifying the specific provisions alleged to have been violated. The controller or processor must then provide the Commission with a written response explaining that the alleged violation did not occur or summarizing how the violation has been cured. If the Commission determines that no violation occurred, the matter would be closed. However, if the Commission determines that the violation has not been cured, it must hold an administrative hearing.

Controllers or processors found to have violated any provision of law may be ordered to cease and desist the violation and/or pay an administrative fine of up to $2,500 for each violation, or up to $7,500 for each intentional violation or violation involving the personal data of a child. If the Commission determines that a violation occurred, the Commission will also determine whether the consumer suffered actual damages as a result of the violation. A consumer found to have suffered actual damages may bring a civil action under the Consumer Protection Act (chapter 19.86 RCW) to obtain injunctive relief and the recovery of actual damages and reasonable

---

48 HB 1850 § 5 (1-3).
49 HB 1850 § 5(8).
50 HB 1850 § 2(1)(a).
51 HB 1850 § 2(4).
52 HB 1850 § 3(1).
53 HB 1850 § 3(6).
54 HB 1850 § 3(3).
55 HB 1850 § 3(4)(a).
56 HB 1850 § 3(4)(b).
57 HB 1850 § 3(4)(c).
58 HB 1850 § 3(5)(a).
59 HB 1850 § 3(5)(b).
Attorney’s fees.\textsuperscript{60} Decisions made by the Commission would be subject to judicial review under an abuse of discretion standard.\textsuperscript{61}

Notably, the Washington Foundational Data Privacy Act would provide a one-year adjustment period between the Commission’s rulemaking activities and subsequent enforcement to allow controllers and processors opportunity to bring their practices into compliance.\textsuperscript{62}

III. Recommendations for Future Legislation

\textit{a. Require a strong opt-in consent model}

We advocate for a strong opt-in consent model as the model which will benefit Washingtonians and potentially have interstate effect. Despite states’ preference for an opt-out or hybrid model, Washington has the opportunity to interrupt the trend and build a structured, transparent standard of consent. Washington has been a leader in technology innovation and is uniquely positioned to influence the national consent standard. While advocates of opt-out consent argue that opt-in frameworks detrimentally affect usability, controllers operating in the EU have adapted to GDPR’s opt-in model, leaning on UX design to innovate strategies for obtaining informed consent. Many companies which operate globally have begun adjusting their standard to that of the GDPR, finding advantage in consistency outweighing any potential drawbacks of an opt-in consent framework. Finally, as we advocate in this paper, a Commission would provide guidance to companies in the U.S. that may have to adapt to an opt-in model. This may be specifically helpful to smaller controllers and processors, who may be more vulnerable to an opt-in model of consent.

\textit{b. Include some form of a private right of action}

Overall, we recommend that any future Washington consumer data privacy law include some form of a private right of action, even if it is limited. A private right of action is an important mechanism for the law to include to enable aggrieved parties to enforce their rights. This especially holds true for parties who may be overlooked by government enforcement regimes, such as historically marginalized groups, as well as for parties who disagree with or do not accept the conclusions reached by the government enforcement regimes, such as potential enforcement via a commission or the AG. With the goal being to ultimately pass a consumer data privacy law, in the spirit of compromise we recommend a bill that places limitations on the private right of action. Remedies can be limited to allow plaintiffs to win injunctive relief, actual or statutory damages, and recovery of attorney’s fees. Exhaustion requirements of an individual first providing notice and an opportunity to cure before bringing suit can also be included. These limitations function to assuage the concerns of opponents of a private right of action, primarily by reducing the number of suits in court, while still offering Washingtonians the benefits of a private right of action.

\textsuperscript{60} HB 1850 § 3(5)(c).
\textsuperscript{61} HB 1850 § 3(6).
\textsuperscript{62} HB 1850 § 8.
c. Leverage the commission as an expert body to guide privacy legislation and build equity into the commissioner appointment process

Investment in the infrastructure necessary to support sophisticated technical regulation and the meaningful enforcement of consumer rights will ensure that the privacy rights of Washingtonians continue to evolve in tandem with technological advancements. However, the implementation and enforcement of these data privacy rights will necessarily be shaped by whose voices are represented in the makeup of the Commission. Therefore, it is imperative to build consumer data privacy infrastructure with a focus on equity from the beginning. Regulators should seek input directly from impacted communities to identify and address their specific concerns.

Additionally, we are concerned about the feasibility of asking three Commissioners to meaningfully represent the interests of all stakeholders – including the legislature, Washingtonians, and controllers and processors of consumer data. Given the diversity of interests represented in the ongoing privacy debate, we suggest that the legislature consider increasing the number of appointed Commissioners and consider designating one a representative of human rights advocacy and one a representative of industry.

To ensure equitable stakeholder representation, we also suggest modifying the process for Commissioner appointment to include a variety of appointment sources that would insulate the Commission from the political influence or control of a single individual. For example, the California Privacy Protection Agency is governed by a five-member board consisting of the chairperson and one other individual appointed by the Governor.\textsuperscript{63} The AG, Senate Rules Committee, and Speaker of the Assembly additionally appoint one member each.\textsuperscript{64} We recommend the Washington Consumer Data Privacy Commission adopt a similar approach to diversify Commissioner appointments.

Finally, we suggest that the appointment process utilize existing governmental equity and human rights divisions, such as requesting input from the Washington State Office of Equity for all Commissioner nominations.

i. Assist controllers and processors in understanding their duties and in coming into compliance with the regulatory framework

In order for the data privacy rights of Washingtonians to be meaningfully protected, covered controllers and processors must be able to feasibly implement and comply with all duties and obligations imposed by future privacy legislation. Research by privacy management software company CYTRIO revealed that as of March 31, 2022, 89% of surveyed medium and large sized companies were either non-compliant or only somewhat compliant with the requirements of the CCPA.\textsuperscript{65} Only 11% of surveyed companies were fully compliant with their CCPA obligations.\textsuperscript{66}

To avoid similar disparities in Washington, the Consumer Data Privacy Commission should take

\textsuperscript{63} CCPA § 1798.199.10.

\textsuperscript{64} CCPA § 1798.199.10.


\textsuperscript{66} Id.
advantage of the one-year gap between the rulemaking process and enforcement provided by HB 1850 to assist controllers and processors in adjusting their practices to come into compliance with their new obligations and duties under a Washington consumer data privacy law. Additionally, we recommend above that the Commission structure be amended to include a representative of the technology industry in the rulemaking process to ensure that any regulations imposed on controllers and processors are informed by technological capabilities and industry best practices.

   ii. Perform consumer outreach to educate Washingtonians about their privacy rights and how to enforce them

Although Washington is a leader in technology and innovation, it is important to remember that Washingtonians possess varying degrees of comfort and sophistication in their technological interactions. Additionally, the potential consequences of data privacy violations are not universal. Consumers belonging to marginalized communities and individuals with limited English proficiency may be particularly vulnerable to unmitigated data harvesting practices. We recommend that the Washington Consumer Data Privacy Commission prioritize consumer education and outreach to ensure that all Washingtonians are aware of their rights as well as potential avenues to enforce them. Specifically, we suggest that the Commission follow the lead of successful governmental educational campaigns to develop comprehensible, consumer-focused guidance.67 These materials should be engaging, regularly updated to reflect developments in relevant areas of the law, and accessible in multiple languages. Finally, the Commission should consider providing annual public-facing reports that outline the landscape of consumer data privacy in Washington to provide accountability and transparency to the people.

IV. Conclusion

We believe the leadership change in Washington’s data privacy legislative debate is an opportunity for legislators to revamp the conversation around consumer data privacy. Legislators have the chance to build a comprehensive data privacy law that provides a framework that benefits all stakeholders. We recommend passing legislation that protects all Washingtonians and considers individuals’ needs in safely navigating online spaces. We believe that structuring regulation to promote transparency, both for consumers to understand their rights and for controllers and processors in understanding how to remain compliant, is the only way to ensure that Washington operates as a leader in technology regulation.

67 See e.g., the Renter’s Handbook provided by the City of Seattle’s Renting in Seattle program https://www.seattle.gov/Documents/Departments/RentingInSeattle/languages/English/RentersHandbook_English.pdf.
Appendix
Character Studies
Case Study A

The Washington State Legislature passes a comprehensive consumer data privacy act that forms a privacy commission with sole enforcement authority. However, the Act excludes a private right of action, and Washington decides to go with an opt-out consent policy, instead of requiring opt-in consent for data collection. How does this affect Washingtonians in their day-to-day interactions with tech?
A proud grandma in Wenatchee who uses Facebook to keep up with family and read the news but is a bit intimidated by technology; gets her news primarily from TV or Facebook and does not use a smartphone.

Mary Fletcher

How will this affect how you interact with technology?

“Well, I don’t really want those Big Tech companies using my data, but I need to see the pictures of my grandkids posted on Facebook, so I’ll probably just go ahead and let them do what they need to in a pinch. Plus, I don’t even know where to begin to ask them to stop doing all that—they always make those web pages so tricky to navigate—guess that’s how they get ya! My granddaughter sent me a news story that explains this commission, I’ll have to ask her more about it.”

Having regularly updated educational materials more readily available in multiple formats may help Mary protect her data and privacy on the Internet.
A weary law student, looking to better understand tech regulation; “My concentration is immigration law, but unchecked data collection and surveillance is a major risk to immigrant communities!”

Jimothy Horses

How will this affect how you interact with technology? “Without default opt-in, I am definitely going to look closely at what data collection practices the company deems necessary to use their product. Maybe I’ll check out what the commission website says about my rights under opt-out. If I don’t trust the company or they want too much data, I’ll try to find an alternative platform? I can’t really do that for things like Lexis and Westlaw though, or any other service that doesn't have viable alternative offerings…”

Data privacy protections could help limit the amount of unmitigated surveillance performed by companies in WA State on consumers of all backgrounds. However, a default opt-out consent model doesn't give consumers full transparency over when they have the right to revoke consent or choice over whatever websites or services to use.
Case Study B

The Washington State Legislature passes a comprehensive data privacy act that establishes a data privacy commission with enforcement power, includes a private right of action, and requires opt-in consent. A mobile game developer has been selling customers' sensitive device data that was collected without their consent. After investigations, hearings and unanswered notices to cure, the WA Data Privacy Commission found reason to believe a violation occurred and determined the consumers of the app had suffered actual damages.
Parent blogger on Bainbridge Island recently elected to her local school board; “I am a proud tech nerd since childhood and am always following the cutting-edge of innovation!”

Will you pursue damages in civil court?

“Finally, some accountability! This mess caused me a lot of trouble. I had to freeze my credit report and change all my cards, so I will definitely be pursuing civil damages and will hopefully recover my legal fees too. While this is great for me, I do worry about the folks who aren’t as up on this as I am or don’t have access to legal services…”

A private right of action will help consumers recover damages for the trouble caused by companies mismanaging their data that refuse to remedy the issue. However, granting the commission with other enforcement powers assures that everyone has access to some form of remedy, no matter their resources.
Harold Fuentes

Compliance Manager at a local tech startup; grew up in Yakima, first in family to attend college. Comfortable with data regulation compliance like GDPR, but otherwise has no formal legal education.

Will you utilize your private right of action?

“I know the regulations from our end enough not to make the same mistake but they’re still pretty confusing since they change all the time, so I wish there was a way to get some official guidance from the folks enforcing it. I’m also not a lawyer, so this private right of action stuff is a little above my head. Maybe I can ask someone in our legal department to help me figure all that out, like where do I begin?”

A commission would help support small to mid-sized companies like Harold’s that are trying to stay in compliance with data privacy protections. It will also help Harold as a Washingtonian consumer to access his rights if he is personally a victim of data misuse.
Regional manager for a major outdoors supply company; “Washingtonian for life! I prefer the PNW air and nature to staring at a device all day.”

Victor Almvig

Will you pursue damages in civil court?

“Ugh, is this the thing I keep getting emails and letters about? I just downloaded that app to find camping spots, I really don’t want to be bothered with all of this. At this point, all of our data has already been leaked in some other data breach, so I just don’t care anymore.”

The feeling of hopelessness faced by so many consumers over companies having free reign over their data has created a sense of futility amongst some folks, which only makes passing these protections more urgent than ever. A commission would have the resources to educate the public on their rights and empower individuals by showing accountability is possible.
Undocumented individual, recently fleeing a domestic violence situation; works for a property management company in Seattle, frequently plays games on her phone and tablet.

Mia Jorgensen

Will you utilize your private right of action?

“I would love to get some sort of compensation for this app selling my data, but I’m nervous to try and go to court with my immigration status. I’ve heard ICE waits at courthouses to try and scoop folks up to deport them—no thanks, not worth the risk.”

While a private right of action is a valuable tool, the reality is that many folks will simply not be able to access it for a variety of reasons, and marginalized communities will continue to be hurt the most. Strengthening state laws around consumer data will also reinforce bills like KWW & COTA that protect immigrant data from being shared with ICE and CBP. A commission devoted to providing resources to every individual in Washington offers an alternative to engaging directly with law enforcement.