February 21, 2019

The Honorable Christine Rolfes, Chair
Members of the Senate Ways and Means Committee
Washington State Senate
311 J.A. Cherberg Building
P.O. Box 40466
Olympia, WA 98504-0466

Re: SB 5376 (Protecting Consumer Data) - OPPOSE

Dear Chair Rolfes and Members of the Senate Ways and Means Committee:

Consumer Reports, Common Sense, Electronic Frontier Foundation, and Privacy Rights Clearinghouse write to oppose SB 5376 (Protecting Consumer Data). Strong, enforceable privacy protections are needed now more than ever, due to the widespread, and largely unregulated, sale of consumer data on the open market. Over the last few years, data tracking practices have become increasingly invasive. Consumers deserve meaningful protections over the collection, retention, and sharing of their personal information, and robust enforcement mechanisms to hold companies accountable. Unfortunately, many of SB 5376's provisions are predicated on fuzzy and debatable notions like "risk" and "compelling business purposes" that fail to protect consumers and don't offer clear guidance to consumers or businesses. Moreover, those assessments will be made in the first instance by companies, who may have a very different interpretation of what is "risky" and "compelling" than ordinary consumers. In addition, businesses' interests are not inherently aligned with the constituents they serve. The undersigned groups opposed this bill as too weak even before a series of new loopholes were inserted to the bill on February 14, making the bill even more indefensible. These include narrowing the scope of personal information covered by the bill and broadening the exemptions for the use of data for advertising purposes. This bill is substantially weaker than privacy legislation recently enacted in California and Europe, and gives companies far too much leeway and control to decide what privacy protections to offer. It should be rejected.

Privacy law should not tether consumer protections to subjective assessments of privacy *risk.* Consumers will always have a privacy interest in data collection, use, retention, or sharing because once private information is in the hands of another there is *always* a chance of some misuse. For example, data collected in the past could be publicly breached, accessed through mandatory legal process, or used for price discrimination to decrease a consumer's share of consumer surplus from any transaction.[1] From the perspective of the consumer, there is *necessarily* privacy risk when someone else has their data. With limited exceptions, a privacy law's protections should not be contingent upon a company's own (and necessarily biased toward its own interests) evaluation of how significant those risks are.

And for this very reason, while the United States has fewer privacy protections than other countries, the laws we have passed have not been artificially constrained by *ad hoc* determinations of privacy risks or harms. The Wiretap Act,[2] for example, does not ask potential eavesdroppers to weigh the relative harms and benefits to determine the legality of intercepting a potential communication. Nor does the Video Privacy Protection Act[3] allow someone to make subjective judgments about how "harmful" the release of someone's viewing habits might be. Rather, the laws' protections apply *per se*, obviating any risk analysis, leading to clearly stronger protections and more clear and predictable rules for everyone.

Because the proliferation of data is, to the consumer, unpredictable and hard to control, the law's protections should apply *per se* protections for privacy intrusions. Potential harms to the consumer may not be obvious when the data is first collected because data collected in the past could be used in new and unexpected ways. In addition, risk assessment introduces unnecessary uncertainty into the law, both for companies and consumers (who might not necessarily agree on what constitutes an acceptable privacy risk).

Furthermore, in practice these risk assessments will be made (often opaquely) by companies with incentives to allow data processing and disregard consumer interests. Companies' profit motives skew their risk calculations from the start. In addition, such assessments will not always be rational: businesses are run by humans, and humans exhibit a natural human tendency to overestimate a small chance of something good happening and to underestimate the chances of something bad happening.[4] This is a core tenet of behavioral economics, and explains why people play the lottery despite the odds and decreasing marginal value of money, or do not

---

[1] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, Future of Privacy Forum Big Data & Privacy Workshop Paper Collection (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.
[2] 18 U.S. § 2511.
[3] 18 U.S.C. § 2710.
[4] Klaus Mathis & Ariel David Steffen, *From Rational Choice to Behavioural Economics*, UNIV. OF LUCERNE (2015) https://www.unilu.ch/fileadmin/fakultaeten/rf/mathis/Dok/1_Mathis_Steffen_From_Rational_Choice_to_Behavioural_Economics.pdf.

buckle their seat belts despite the low cost and tremendous risk. Translated to data privacy, companies will tend to undervalue data security, and undervalue data minimization as well, discounting the likelihood of a security event, but overly optimistic about the potential for found wealth in data troves. Therefore, privacy law should reflect the reality of human nature, and eliminate opportunities for skewed incentives and irrational tendencies to weaken privacy protections.

Landmark legislation such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) give consumers better access to and greater control over the uses of their personal information. While that is also a claimed goal of this bill, it is substantially more flimsy than both pieces of legislation. For example, while SB 5376 purportedly extends to consumers the right to opt out of the disclosure of their information, unless that information is sold for direct marketing, the company selling—and profiting—from that data can decline the consumer's request if there is a "compelling business purpose." This term is not defined by the bill, leaving companies to decide themselves whether or not to extend these protections to consumers. Instead, companies should be required to have reasonable reasons for the collection and use of data, as part of providing the service requested by the consumer.

Similarly, the bill gives consumers opt-in protections for data processing practices (which could include data collection, sharing, or sale) that are deemed "risky." However, it is up to the company to decide whether or not a practice is risky—rendering these protections essentially voluntary. Companies have proven that they cannot be trusted to regulate themselves with respect to privacy. The online advertising industry has already reneged on commitments to honor Do Not Track signals and have implemented self-regulation practices that have failed to limit the collection and sale of consumer data in any meaningful way.[5] If passed, this legislation could do real harm by enshrining existing weak, voluntary controls into law.

This bill also lacks strong enforcement mechanisms to hold companies accountable for wrongdoing. The enforcement provision includes "right to cure" language, which prevents the Attorney General from taking enforcement action if the company, after being notified, complies with the law within 30 days. Not only would such language excessively tax the Attorney General's office—forcing it to waste time building cases that go nowhere—it lets companies get away with bad behavior until they're caught. Making matters worse, the AG must then pursue the uncertain debate about what is "risky" and "compelling." This is bad public policy, and should be immediately deleted from the bill. Instead, the bill should include a private right of action, which would give companies sufficient incentives to comply.

---

[5] *Understanding the Digital Advertising Ecosystem, Hearing Before the House Subcommittee on Digital Commerce and Consumer Protection* at 10 (2018) (Statement of Justin Brookman), https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-Wstate-BrookmanJ-20180614.pdf.

In addition, privacy legislation should address data collection, requiring companies to engage in reasonable data minimization. Under this bill, consumers are given the right to opt in to data collection only if companies themselves deem the practices "risky." Instead, companies simply should be required to collect and retain data only as reasonably necessary for services requested by a consumer. After years of countless data breaches and privacy scandals, consumers are extremely worried about excessive data collection and sharing.[6] Public policy should step in to accord companies' data collection, retention, and sharing practices to reasonable consumer expectations—not to companies' subjective determination of their own interests and consumers' risks.

Finally, this bill outlines several consumer protections with respect to the use of facial recognition technology. However, these proposals will do little to meaningfully rein in misuse of this technology. For example, while the bill purportedly requires consumer consent to the use of facial recognition technology, it actually allows companies to substitute notification for seeking consent—leaving consumers without a real opportunity to exercise choice or control. This technology has the potential to significantly increase companies' ability to track consumers as they move through their everyday lives and combine it with other information collected and sold about them, compromising consumer privacy and autonomy. Biometric data is highly personal and subject to significant misuse; consumers deserve strong protections over its collection and use.

Washington State has a real opportunity to be a leading state on privacy issues. Inadequate federal controls have left companies to their own devices for years, incentivizing them to develop incomprehensible, broadly-drafted privacy policies that shield them from liability for outrageous practices—leaving consumers little choice but to submit to misuse of their data, or else miss out on essential and useful services. It's time for this unregulated data collection and misuse to end, and this legislation will not achieve those goals. Please reject this legislation.

Sincerely,

Consumer Reports
Common Sense
Electronic Frontier Foundation
Privacy Rights Clearinghouse

[6] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, CONSUMER REPORTS (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data/.