March 25, 2019

The Honorable Zack Hudgins, Chair
Members of the House Innovation, Technology & Economic Development Committee
205A John L. O'Brien Building
P.O. Box 40600
Olympia, WA 98504-0600

Re: Protecting Consumer Data (ITED v. 4) - OPPOSE

Dear Chair Hudgins and Members of the Committee:

Consumer Reports, Consumer Federation of America, Digital Privacy Alliance, Electronic Frontier Foundation, Privacy Rights Clearinghouse, and WashPIRG urge you to oppose the general privacy legislation currently being considered by the Washington State legislature through the vehicle of ITED v. 4. While ITED v. 4 does not suffer from some of the more outrageous problems found in the version that passed the Senate (SB 5376)—notably predicating most consumer rights on subjective assessments of privacy "risks" and company "interests" by the regulated companies themselves—it is still too weak, and has too many exceptions and too few specifics to protect Washingtonians' privacy. In order to offer meaningful protections, the bill must be strengthened to bring it *at least* to the standard of the California Consumer Privacy Act (CCPA). Washingtonians have a right to privacy, and deserve strong protections over the

collection, retention, and sharing of their personal information, and robust enforcement mechanisms to hold companies accountable. We recommend that the bill be amended to:

- Eliminate requirements that opt-out requests be subject to verification;
- Eliminate loopholes that could be interpreted broadly to weaken consumer rights;
- Require reasonable data minimization instead of risk assessments to determine when consent is needed;
- Have a strong definition of deidentified data that mirrors the Federal Trade Commission's; and
- Provide strong enforcement that doesn't allow businesses a get-out-of-jail-free card before being held accountable, and add a real private right of action.

We also strongly urge that weaknesses in the Senate bill *not* be incorporated into the House version, including:

- A provision allowing companies to deny rights if there are "legitimate grounds" to do so;
- Weak regulations on facial recognition that don't require meaningful consent for its use and don't require third-party testing of these technologies for bias and accuracy.

Both the House and Senate bills are, in their current versions, substantially weaker than privacy legislation recently enacted in California and Europe. If not drastically improved, they should be rejected, as they set a dangerous precedent for privacy legislation nationally and in the states.

Eliminate requirements that opt-out requests be subject to verification.

Section 6(6) gives consumers the right to opt out of processing, which means "any collection, use, storage, disclosure, analysis, deletion, or modification of personal data."[1] But it sets an unacceptably high bar for these requests by subjecting them to verification by the company—requiring companies to "reasonably authenticate the request and the consumer making the request using reasonable means."[2] Thus, companies could require that consumers set up accounts in order to exercise their rights under the law—and hand over even more personal information. Consumers shouldn't have to verify their identity, for example by providing a driver's license, in order to opt-out of targeted advertising. Further, much of that data collected online (including for targeted advertising) is tied to a device and not an individual identity; in such cases, verification may be impossible, rendering opt-out rights illusory. In contrast, the CCPA explicitly states that

[1] Sec. 3(19).

[2] Sec. 3(24). Furthermore, an opt-out regime can only work if consumers can opt out universally with simple tools—such as platform-level Do Not Track instructions—that companies should be obligated to honor. Opting out site by site, store by store is not practical. The CCPA accommodates this by giving the Attorney General the right to establish sensible rules to guide the process for submitting opt-out requests and businesses' compliance with those requests, and by declining to require authentication for these requests.

companies "shall not require the consumer to create an account with the business in order to make a verifiable consumer request," and pointedly does not tether opt out rights to identity verification.[3]

Eliminate loopholes that could be interpreted broadly to weaken consumer rights.

ITED v. 4 is filled with exceptions that would leave consumers without adequate privacy protections. Section 6, which purports to give consumers the right to restrict processing, such as the disclosure of their information to third parties, has a number of potential loopholes that need to be closed. Section 6(6), for example, gives consumers the option to restrict processing, but only if it meets one of four criteria, including if it is "[i]nconsistent with a purpose for which the personal data was collected." This is vague and arguably means that so long as a purpose is mentioned in a privacy policy, opt-out rights don't apply. Furthermore, the opt-out to processing in Section 6(8) could be interpreted to only apply to the transfer of data for targeted advertising and direct marketing, leaving out other forms of sharing, for example for research and development purposes. There is a separate long list of exemptions from opt-out processing rights in Section 11, such as for public health research, security, and research in the public interest, that are too broad. Unlike the CCPA, these exceptions aren't limited to what is reasonably necessary to accomplish those goals.

The definition of targeted advertising itself has too many exemptions—for example, the exemption for "advertising to a consumer based upon the consumer's visits to a web site, application, or online service that a reasonable consumer would believe to be associated with the publisher where the ad is placed based on common branding, trademarks, or other indicia of common ownership, or in response to the consumer's request for information or feedback"[4] is confusing and could be interpreted to allow retargeting and other practices that should reasonably be covered by the opt-out. And, the "direct relationship" carve-out from the definition of sale—exempting disclosures to third parties with whom the consumer has a direct relationship "for the purposes of providing a product or service requested by the consumer *or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data*" (emphasis added)—is potentially too expansive, further weakening the right to opt-out of processing.[5]

There are additional exemptions that could undermine consumer rights. For example, the right to delete in Section 6(4) is quite limited and applies only in certain circumstances, for example, if the consumer withdraws their consent for the controller to process their information and "there are no other legitimate grounds for processing." Instead, the right to delete should presumptively

[3] 1798.130(a)(2).
[4] Sec. 3(28).
[5] Sec. 3(26)(b).

apply to all consumer data, with only specific and justified exemptions. The definition of "business purposes" is also far too broad, with undefined exemptions such as "research" that could be exploited—this is significant, because uses of data for business purposes are generally exempted from the opt-in to processing for risky data outlined in Section 9.[6] Finally, the Section 17 preemption language is too extensive, broadly preempting all local privacy laws, ordinances, and regulations, potentially preempting even those not related to online privacy, such as anti-stalking ordinances.

Require reasonable data minimization instead of risk assessments to determine when consent is needed.

Both bills give consumers opt-in rights to processing if, after a risk analysis, the company decides that certain forms of processing are "risky."[7] Rights shouldn't be conditional on subjective analyses by businesses. Instead, people should have privacy protections by default. Consumers deserve data minimization, meaning that companies are required to limit their data collection to the information that is reasonably necessary to operate the service requested by the consumer, in addition to greater control over data sharing. This is a more protective formulation from the opt-out model. For example, we recommend replacing the risk assessment provisions in Section 9 of the House version (Section 8 of SB 5376) with language similar to the following:

(a) Subject to (c)-(f), a business that collects a consumer's personal information shall limit its collection and sharing of personal information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention.
(b) Subject to (c)-(f), a business that collects a consumer's personal information shall limit its use and retention of personal information to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a related operational purpose, provided that data collected or retained solely for security or fraud prevention may not be used for related operational purposes.
(c) Other than as described in (a)-(b), a business shall not collect or share a consumer's personal information unless the consumer has affirmatively authorized the collection or disclosure. This right may be referred to as "the right to opt-in consent."
(d) A business shall request a user's opt-in consent separately from any other permission or consent, with the option to decline consent at least as prominent as the option to provide consent.
(e) If a consumer declines to provide their opt-in consent to the disclosure of their personal information, the business shall refrain for at least 12 months before again requesting that the consumer provide their opt-in consent to the disclosure of their personal information. The business may however make available a setting or other user control that the consumer may affirmatively access in order to consent to additional data collection or sharing.

[6] Sec. 3(3).
[7] Sec. 9.

(f) A business that obtains a consumer's opt-in consent to collect or disclose their personal information pursuant to this section shall provide consumers the ability to withdraw such consent through a readily usable and automated means at anytime.

No reasonable person would want the most sensitive, personal information about them sold to strangers without their knowledge, and companies should be required to honor that as a matter of course.

Privacy legislation should have a strong definition of deidentified data that mirrors the Federal Trade Commission's.

Because deidentified data is not subject to the privacy provisions of the bill, and because, without appropriate controls, deidentified data can be relinked to consumers, strong protections are needed to ensure that it remains in deidentified form. Unfortunately, both bills lack strong standards for deidentification. They allow companies to make subjective risk assessments, for example, rather than requiring companies to ensure the data is deidentified, the company may determine "that the risk of reidentification is small." Furthermore, SB 5376 does not explicitly require companies to place contractual controls over downstream recipients.[8] In contrast, the Federal Trade Commission (FTC) outlines a strong framework for deidentified data that 1) requires the company to take reasonable measures to ensure that the data is deidentified; 2) to publicly commit to store and use it in a deidentified fashion, and not attempt to reidentify; and 3) prohibit downstream recipients by contract from reidentifying the data.[9] We urge legislators to revise the definition of deidentification based on the FTC's model.

Privacy legislation should provide strong enforcement that doesn't allow businesses a "get out of jail free" card before being held accountable, with a real private right of action.

Legislators should eliminate language that lets companies off the hook for wrongdoing ("right to cure" provisions) and include a real private right of action, thereby ensuring that companies have sufficient incentives to comply. For example, we recommend the following language for Section 14 of the House draft (and Section 12 of SB 5376):

> (a) A consumer who has suffered a violation of this Act may bring a lawsuit against the business that violated this Act. A violation of this Act shall be deemed to constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this Act.
> (b) A consumer who prevails in such a lawsuit shall obtain the following remedies:
> (1) Damages in an amount not greater than seven hundred and fifty dollars ($750) per consumer

[8] Section 3(10)(b).

[9] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Fed. Trade Comm'n at 21 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

per incident or actual damages, whichever is greater.
(2) Injunctive or declaratory relief, as the court deems proper.
(3) Reasonable attorney fees and costs.
(4) Any other relief the court deems proper.
(c) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.
(d) A consumer bringing an action shall notify the Attorney General within 30 days that the action has been filed.[10]

Both bills include "right to cure" language, which prevents the consumer or Attorney General from taking action if the company, after being notified, complies with the law within 30 days. This language is particularly harmful in the context of AG enforcement. This language would excessively tax the Attorney General's office—forcing it to waste time building cases that go nowhere. Making matters worse, the AG must then pursue the uncertain debate about what is "risky" and "legitimate." This is bad public policy, and should be immediately deleted from the bill.

Finally, SB 5376 contains even more objectionable language than ITED v. 4. We strongly urge legislators to:

Reject language that allows companies to deny rights if there are "legitimate grounds" to do so.

The Senate version of the bill is unacceptable: it purportedly extends to consumers the right to opt out of the disclosure of their information, but 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 "legitimate ground" to do so.[13] This term is not defined in the bill, giving companies far too much leeway to determine whether to extend protections to consumers.

---

[10] Adapted from the California Consumer Privacy Act, 1798.150.
[11] RCW 19.86.093, https://app.leg.wa.gov/RCW/default.aspx?cite=19.86.093.
[12] Carolyn L. Carter, *Consumer Protection in the States: A 50-State Report on Unfair and Deceptive Acts and Practices Statutes*, National Consumer Law Center at 29 (Feb. 2009), http://www.nclc.org/images/pdf/udap/report_50_states.pdf.
[13] Sec. 6(c).

After years of countless data breaches and privacy scandals, consumers are extremely worried about excessive data collection and sharing.[14] Public policy should step in to accord companies' data collection, retention, and sharing practices to strong standards—not to companies' subjective determination of their own interests and consumers' risks.

Reject weak regulations on facial recognition that don't require meaningful consent for its use and don't require third-party testing of these technologies for bias and accuracy.

In considering legislation related to facial recognition technologies, we urge extreme caution: inadequate controls could have the effect of condoning and encouraging its spread without addressing serious concerns about privacy and disparate impact. SB 5376 would not adequately rein in misuse of facial recognition technology. For example, while the Senate 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.[15] Biometric data is highly personal and subject to significant misuse; consumers deserve strong protections over its collection and use.

Any facial recognition legislation should include meaningful consent for the use of these technologies and require companies to engage in third-party testing for racial, ethnic, and gender biases and accuracy. This is important, because these technologies are more likely to misidentify women and people of color at higher rates.[16] Companies must be required to have these processes tested by disinterested, independent researchers who don't have a financial stake in the outcome. Finally, adequate oversight and regular, timely analyses from the Office of Privacy and Data Protection related to the impact of these technologies are essential.

Conclusion

Strong privacy legislation requires data minimization and privacy-by-default. For example, companies should be required to collect, retain, and share data only as reasonably necessary for services requested by a consumer, and not leave it to the consumer to figure out how to protect their own privacy. At the very least, Washingtonians should have clear opt-out rights like in the

---

[14] 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/; "Nearly two-thirds of all Americans (64%) have at least one online account that holds their health, financial or other sensitive personal information. And a similar share (64%) have experienced or been notified of a significant data breach pertaining to their personal data or accounts. More broadly, roughly half the public feels their data have gotten less secure in recent years. Any many Americans express a lack of confidence in various institutions – most notably, the federal government and social media platforms – to safeguard and protect their personal information." Aaron Smith, *Americans and Cybersecurity*, Pew Research Ctr. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/1-americans-experiences-with-data-security/.

[15] Sec. 14(4).

[16] Brendan F. Clare et al., *Face Recognition Performance: Role of Demographic Information*, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, Dec. 2012.

California Consumer Privacy Act—that are guaranteed by law, not subject to obscure balancing. Washington State has a real opportunity to be a leader on privacy issues. We look forward to working with you to enact privacy legislation that puts consumer privacy first.

Sincerely,

Consumer Reports
Consumer Federation of America
Digital Privacy Alliance
Electronic Frontier Foundation
Privacy Rights Clearinghouse
WashPIRG