HB 1850 Feedback

by the American Civil Liberties Union of Washington. Wednesday, Jan. 19, 2022. Bill Prefiled Friday, Jan. 7, 2022

This feedback draws upon prior feedback provided by the ACLU of Washington (attached) and Consumer Federation of America on SB 5062 in 2021. Because HB 1850 is based on SB 5062, much of the feedback is similar. There are some strong provisions in HB 1850.

- **A private right of action with damages.** A private right of action is important to give consumers power to hold companies that violate their rights accountable. However, to make this provision operationally meaningful, we strongly recommend strengthening this section to remove the right to cure and include a minimum per violation penalty and coverage of attorney's fees.
- **The creation of a funded privacy commission.** Creating an agency dedicated to enforcing people's privacy rights and providing guidance on privacy would likely be beneficial. We recommend strengthening this provision by ensuring that the enforcement interaction between the commission and the attorney general is clarified and stronger revolving door protections are put in place.
- **The creation of a consumer privacy account.** Creating an account only to be used for the purposes of recovery of costs and attorney's fees accrued by the attorney general in enforcing this bill and for the privacy commission would likely be beneficial.

However, the vast majority of the bill's provisions are nearly identical to SB 5062. HB 1850:

- **Does not require opt-in consent to collect, use, and share all data.** As written, this bill only requires affirmative consent for narrowly defined category of "sensitive data" but not for any other data, leaving a massive trove of data inadequately protected. All data is "sensitive." Even ostensibly innocuous and "non-sensitive" data such as shopping history 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. People's information should remain private *unless* an entity receives freely given, specific, informed, unambiguous opt-in consent to collect, use, and share their personal information.
- **Allows companies to track and profile consumers without their consent.** The loopholes in the definition of targeted advertising allow for companies to track and profile consumers without their consent, though consumers may opt out of *seeing* the targeted ads. It also allows for companies like Google and Facebook to track, profile, and display ads to consumers without their knowledge or consent. Additionally, the right to opt out of profiling is severely limited by the qualifier, "in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer." With this

Eric González Alfaro, *Legislative Director*|egonzalez@aclu-wa.org| www.aclu-wa.org

ACLU Washington

language, consumers do not have the right to choose not to be profiled and have assumptions made about them, unless those assumptions would have some kind of legal or significant effect on them. Additionally, it would be up to the controller to determine whether or not instances of profiling have legal or significant effects.

- **Allows companies to sell consumers' personal information to affiliated companies without a consumer's knowledge or consent.** The definition of "share" exempts sharing consumers' personal information with affiliates. Companies are increasingly merging with and acquiring other companies, which in many cases are in completely different lines of business. Consumers often have no idea of who these affiliates are or what they do. Exempting affiliates would deny consumers the ability to prevent their data from being shared with affiliates that may use their data for unrelated lines of business without their knowledge or consent.
- **Denies consumers any right to protect their social media data if they did not restrict that data to a specific audience.** The exemption in the definition of "share" for the disclosure of information consumers intentionally made on a channel of mass media and did not restrict to a specific audience denies consumers the ability to prevent that information from being collected and shared for commercial purposes. The fact that consumers shared information on a social media platform does not mean that they anticipated that information would be sold, nor does their failure to restrict their data to specific audiences mean that they intended it to be "fair game" for such practices.
- **Undermines consumers' ability to access and obtain their data.** The opt-out framework of this bill undermines consumers' ability to access and obtain data that a controller may have obtained from a data broker or other sources.
- **Restricts consumers' right to correct inaccurate data.** The right to correct inaccurate personal data is qualified by the vague phrase, "taking into account the nature of the personal data and the purposes of the processing of the personal data." This vague qualifier would allow companies to deny a consumer's right to correction for virtually any reason.
- **Allows for warrantless data sharing with law enforcement.** This bill contains an exemption allowing for controllers or processors to warrantlessly share personal data with law enforcement. Consumers' data should not be provided to law enforcement without a court order or similar due process, unless they give consent.
- **Preempts local jurisdictions from passing stronger privacy protections.** Local jurisdictions should be able to provide stronger privacy protections for their residents.
- **Gives data controllers power to move data into different categories with different protections.** Allowing covered entities to move data in and out of different categories, which are subject to different rules, makes tracking and controlling personal data more difficult, if not impossible for consumers. Controllers could justify hiding the data it has about consumers by declaring that the data is pseudonymous, then process that data as identifiable data when convenient.

- **Limits the attorney general's ability to enforce the privacy violations with a "right to cure" provision.** This provision significantly impedes the attorney general's ability to obtain remedies for consumers. Additionally, there is no definition or guidance as to what constitutes a cure.
- **Does not adequately protect children's privacy.** By including protections only for "known child[ren]," the controller would only have to allow the parent or legal guardian to act on the child's behalf if the controller knew that the consumer was a child when the personal data was processed. A parent or legal guardian should be able to protect their child's privacy and exercise privacy rights, regardless of whether the controller knew the consumer was a child.
- **Does not require consent to use people's data for research**. Controllers are able to use or sell consumers' data for research based solely on its own risk-benefit analysis without obtaining consent.
- **Allows companies to avoid responsibility for sharing data with third parties.** Controllers and processors bear no responsibility if the third parties to which they disclosed consumers' data violate the law if they "did not have actual knowledge" that those parties "intended to commit a violation." The requirement to prove that controllers or processors had "actual knowledge" that the recipient of the data intended to commit a violation is a near impossible burden of proof to meet.
- **Exempts nonprofits organizations; institutions of higher education including for-profit-institutions, employment data, and personal data covered by some federal laws.** Nonprofits organizations and institutions of higher education collect, use, and share large quantities of personal data that should be covered, and there is no reason to exempt personal data covered by other laws, when the privacy protections of those laws are much weaker and do not preempt stronger laws.
- **Contains a number of other significant loopholes in its definitions, qualifying language, and overbroad exemptions.**

Following is a detailed analysis of HB 1850 and our recommendations.

Section 3: Definitions

"Consent" This definition describes "consent" as a "freely given, specific, informed, affirmative, and unambiguous indication of the consumers wishes by which the consumer signifies agreement to the processing of personal data related to the consumer for a narrowly defined particular purpose." In this bill, consent is only required to process "sensitive" information about consumers. The passive language used in this definition allows for consent to be satisfied simply by a person clicking through a long and obscure privacy notice that they did not read.

Recommendation: We recommend modifying the definition to read: "Consent" means freely given, specific, informed, unambiguous, opt-in consent by consumers to allow specific personal data related to the consumer to be processed for a narrowly defined purpose that is clearly

described to the consumer before such agreement is sought. Agreement obtained through dark patterns does not constitute consent."

"Consumer" This definition excludes employment data by stating "It does not include a natural person acting in a commercial or employment context."

Recommendation: We recommend modifying the definition to read: "Consumer" means a natural person who is a Washington state resident. The location of a person in Washington state shall create a presumption that the person is a Washington state resident.

"Deidentified data" The definition of deidentified data should be strengthened to ensure that controllers may not move massive amounts of data to a lower tier of protection, and should prevent controllers from changing their mind down the line to bring that trove of data back to the identifiable category.

Recommendation: We recommend modifying this definition to read: "Deidentified data means data that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual or household, provided that a controller that uses deidentified data must: (a) implement technical safeguards that prohibit reidentification of the data; (b) implement business processes that specifically prohibit reidentification of the data; (c) implement business processes that prevent inadvertent release of deidentified data; (d) not attempt to re-identity the information; and (e) contractually obligate any recipients of the information to comply with all the provisions of this subsection. If a controller intentionally shares any deidentified data, it shall condition such sharing on the agreement by any recipients to abide by the same restrictions and to submit to jurisdiction under this chapter in any action based on violation of such restrictions."

"Personal data" This definition is too narrow and excludes "publicly available information." This has the effect later of meaning that the consumer cannot discover what publicly available data the controller is processing as part of the larger data set.

Recommendation: We recommend it read: "Personal data means any information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to a particular individual, household, or device. Information is reasonably linkable to an individual, household, or device if it can be used on its own or in combination with other information to identify an individual, household or device."

"Pseudonymous data" This definition is not necessary because data that cannot be used to identify the consumer is already covered in the definition of deidentified data. If additional information were added to deidentified data, allowing for that data to be attributed to a specific natural person, the data would no longer be deidentified. Additionally, separate storage would not be an effective means of protecting data as controllers would have the discretion to change data categories at their will.

Recommendation: We recommend removing this definition and references to it in the text of the legislation.

"Share," "shared," or "sharing" This definition excludes coverage of processors, affiliates, social media data, employment data, and more. These loopholes significantly undermine people's privacy rights. Companies are increasingly merging with and acquiring other companies, which in many cases are in completely different lines of business. Consumers often have no idea of who these affiliates are or what they do. Exempting sharing with affiliates would deny consumers the ability to prevent their data from being used for unrelated purposes by businesses they do not know without their knowledge or consent. Additionally, the exemption for information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience is concerning. This exemption would deny consumers the ability to prevent their personal data from being collected from sources such as social media and shared for commercial purposes. The fact that consumers posted information on a social media platform does not mean that they anticipated such collection and sharing, nor should their failure to restrict their data to specific audiences be construed to mean that they intended their information to be "fair game" for such practices.

Recommendation: To fix these loopholes, we recommend modifying the definition to read: "Share," "shared," or "sharing" means any action, set of actions, or omission in which a covered entity, data processer, controller, third party, or affiliate makes personal information available to any other entity, intentionally or unintentionally, including but not limited to sharing, publishing, selling, renting, releasing, disclosing, disseminating, making available, transferring, leasing, providing access to, failing to restrict access to, or other communicating orally, in writing, or by electronic or other means."

"Sensitive data" Even ostensibly innocuous and "non-sensitive" data such as shopping history 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. As written, this bill only requires consent for narrowly defined "sensitive data" but not for any other data, leaving a massive trove of data inadequately protected. All data is "sensitive" so a distinct category of separately protected data is not necessary.

Recommendation: We recommend that this definition and category of data be removed entirely from the bill, as all data can be deemed "sensitive."

"Targeted Advertising" Because targeted advertising is defined as *displaying* ads based on tracking and profiling consumers, consumers' rights to opt out of targeted advertising means they can only opt out of certain ads being *displayed* to them, not out of being tracked and profiled. Even if consumers opt out, companies can continue tracking and profiling them and use the data for purposes beyond advertising, constrained only by some narrow provisions in the bill having to do with sensitive data and profiling that results in certain legal effects. Additionally, this definition completely excludes advertising that is based on tracking consumers over time on a controller's own websites or online applications. This loophole allows for companies such as Google or Facebook to continue doing business as usual—profiling consumers based on their activities on their websites and applications over time and profit by serving consumers targeted advertisements on behalf of other businesses. This loophole further limits consumers' already

limited right to opt out of targeted advertising in Section 5 by not allowing them to opt out of advertising practices of companies like Google and Facebook.

Recommendation: We recommend modifying this definition to read: "Targeted advertising" means the act of obtaining information about a consumer to direct or display an advertisement to a consumer that is selected based in whole or in part on personal data about the consumer. It does not include displaying advertisements to a consumer based solely upon the consumer's current visit to a website, application, service, or covered entity, or in direct response to the individual's request for information or feedback."

Section 4: Jurisdictional Scope

Sec. 4(2) Nonprofits organizations and institutions of higher education collect, use, and share large quantities of personal data that should be covered. Additionally, there is no reason to exempt personal data when federal laws do not prevent states from providing stronger protections. For example, the Gramm-Leach-Bliley Act (GLBA) only provides consumers the ability to opt out of their data being disclosed to third parties. There are no rights regarding targeted advertising, no rights to correct, delete, or port data, and no civil rights protections. There is no reason to exempt GLBA when it provides weaker privacy rights and does not preempt states from implementing stronger privacy protections.

Recommendation: We recommend removing the exemptions for nonprofit organizations, institutions of higher education (especially as many institutions of higher education are for-profit institutions), employment data, and personal data covered by some federal laws.

Sec. 4(1)(a) and (b) Additionally, the current threshold to be considered a covered entity is very high and excludes many businesses that collect, share, and use people's information.

Recommendation: We recommend lowering the threshold of 100k consumers and removing the second requirement to be considered a covered entity (derive over 25% of gross revenue from the sharing of personal data and control or process personal data of 25,000 consumers or more). It is likely difficult to calculate what revenue is from the sale of personal data and may lead to confusion and inconsistencies in reporting/enforcement of covered entities.

Section 5: Consumer Rights

This section contains many loopholes that undermine consumer rights.

Sec. 5(1) This gives consumers the right to confirm whether the controller is processing their personal information and, if so, to access it, but it should make clear that consumers are entitled to see the specific pieces of personal information that are being processed. Additionally, this right is undermined by the bill's opt-out model which puts the onus on consumers to ask businesses whether they are processing their data.

Recommendation: To make this right meaningful, we recommend creating an opt-in consent requirement for all data and modifying the language to read: "A consumer has the right to know what personal data a controller is processing about the consumer, if any, including the categories and specific pieces of information being processed."

Sec. 5(4) The right for a consumer to obtain the data a controller has about them is limited to the personal data the consumer previously provided to the controller, which is a significant loophole. This loophole restricts consumers from accessing the data that a controller may have obtained from a data broker or other sources. It is unclear whether consumers would have the right to access and obtain data about profiles that have been created about them from their activities as they did not necessarily "provide" that data to the controller.

Recommendation: We recommend modifying the language to read: "The right to access and obtain the consumer's personal data processed by a controller, in a machine-readable format that allows a consumer to transfer their personal information from one entity to another entity without hindrance." Again, we recommend modifying the definition of personal information so that it includes publicly available information. Otherwise, consumers will not be able to know about, access, obtain, correct, or delete some information collected by data brokers.

Sec. 5(2) The right to correct inaccurate personal data is qualified by the vague phrase, "taking into account the nature of the personal data and the purposes of the processing of the personal data." This vague qualifier would allow companies to deny a consumer's right to correction for virtually any reason.

Recommendation: We recommend modifying this language to read: "A consumer has the right to correct inaccurate personal data."

Sec. 5(5)(a) As previously noted, the right to opt out of targeted advertising is limited by the definition of targeted advertising not including the acts of profiling and targeting themselves. Additionally, the definition would exclude companies that conduct targeted advertising based on tracking consumers over time on their own websites or online applications, so would effectively exclude some of the largest companies, including but not limited to Google and Facebook.

Recommendation: As stated above, we recommend modifying the definition of "targeted advertising" to eliminate loopholes and we recommend requiring opt-in consent for any targeted advertising.

Sec. 5(5)(b) As previously noted, the right to opt out of the sharing of personal data does not apply to sharing with affiliates.
Recommendation: As stated above, we recommend modifying the definition of "sharing" and requiring opt-in consent for any sharing of personal data.

Sec. 5(5)(c) The right to opt out of profiling is limited to when profiling is used "in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer." With this language, consumers do not have the right to choose not to be profiled and have assumptions made about them, unless those assumptions would have some

kind of legal or significant effect on them. Additionally, it would be up to the controller to determine whether or not instances of profiling have legal or significant effects. Consumers should have the right to refuse consent to be profiled.

Recommendation: We recommend modifying the language to read: "A consumer has the right to refuse consent for any processing of the consumer's personal data that is not essential to the primary transaction."

Section 6: Exercising Consumer Rights

Sec. 6(3) An issue with including protections only for "known child[ren]" is that companies may think the best practice is to avoid gaining knowledge in the first place. The term "known child" could be construed to mean that the controller would only have to allow the parent or legal guardian to act on the child's behalf if the controller knew that the consumer was a child when the personal data was processed. A parent or legal guardian should be able to protect their child's privacy and exercise privacy rights, regardless of whether the controller knew the consumer was a child.

Recommendation: We recommend modifying the language to read: "In the case of processing personal data of a child, the parent or legal guardian of the child may exercise the rights of this chapter on the child's behalf."

Sec. 6(4) This provision only allows guardians, conservators, and others who have "protective arrangements" concerning consumers under state law to exercise consumer rights on their behalf, but does not describe others whom consumers may authorize to act on their behalf. Consumers may need or want to ask for help managing their privacy from a relative, friend, volunteer, social worker, health aide, or a consumer protection agency.

Recommendation: We recommend modifying the language to read: "Consumers may designate agents to exercise their privacy rights on their behalf, and as long as reasonable verification is provided, the controller should honor the agents' request."

Section 7: Responding to Requests

Sec. 7(4)(d) This provision exempts controllers from complying with a consumer request to exercise their rights if the controller is unable to authenticate the request using commercially reasonable efforts. If the controller fails to put an "authentication" mechanism in place, it should not be able to use that fact to avoid complying with consumers' rights.

Recommendation: We recommend adding the following language: "Controllers shall make an authentication mechanism clearly accessible and usable by consumers seeking to exercise their rights."

Sec. 7(5)(a) This provision states that controllers must establish an internal process whereby consumers may appeal a refusal by the controller to fulfill a person's data privacy rights. This process has no third-party visibility or outside engagement and may allow companies to create

barriers for people trying to exercise their rights. Additionally, a written explanation of why a person has been denied their data rights does not provide sufficient transparency and accountability.

Recommendation: This provision highlights the importance of having a strong private right of action that has a minimum per violation fee and includes attorney's fees, and we recommend including such a private right of action in the enforcement section.

Section 8: Responsibility According to Role

Sec. 8(2)(a), (2)(b), and (4) The qualifying phrases, "taking into account the nature of the processing" and "insofar this is possible" make it unclear who is responsible for making the determination about the nature of the processing.

Recommendation: We recommend removing these qualifying phrases.

Section 9: Responsibilities of Controllers

Recommendation: We recommend substituting this entire section with the language from Section 5 of HB 1433.

Sec. 9 This section could benefit from stronger language and a requirement for a state agency to develop model privacy notices that are as easy as possible for people to read and understand. The agency should be instructed to develop standardized wording for information required to be provided to consumers about the categories of personal data, the purposes for which the data will be processed, and the categories of third parties with which the data are shared.

Sec. 9(1)(b) As stated above, controllers should not be able to share consumers' data with third parties (including affiliates) or use data for any purpose unless they have obtained affirmative opt-in consent.

Sec. 9(5) Controllers should meet or exceed applicable industry standards, which are designed to help businesses ensure that they do the best job possible to protect the confidentiality, integrity, and accessibility of the data they hold.

Sec. 9(7) This important provision prohibits discrimination against a consumer for exercising their rights, including by denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. It would not prohibit controllers from participating in loyalty, rewards, or discount programs. The language here could allow for loyalty programs that share information with third parties, which creates pay-for-privacy concerns.

Sec. 9(8)(a) This provision prohibits the processing of "sensitive data" without the consumer's consent, or in the case of "known child," the parent's or guardian's consent. As described above, the use of the term "known child" raises concerns. The Children's Online Privacy Protection Act (COPPA) apply to "any operator of a Web site or online service directed to children, or any

operator that has actual knowledge that is collecting or maintaining personal information from a child." COPPA applies when a website or online service is directed to children even if the operator does not actually know that the consumer is a child because it is a reasonable assumption, and doing otherwise would create a huge loophole that would endanger children's privacy and make enforcement very difficult. In the online context, the bill should mirror the language of COPPA. In offline situations the bill could require controllers to take reasonable steps to refrain from collecting personal data about children without parents' or guardians' consent. Even better, Washington could simply prohibit collecting children's personal data, online and offline.

Sec. 9(10) This provision states: "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter is deemed contrary to public policy and is void and unenforceable." Including "terms of service" to the beginning of this sentence would strengthen this provision as many interactions between customers and businesses are not governed by contracts or agreements, but rather by terms of service.

Section 10: Processing Deidentified Data or Pseudonymous Data

Recommendation: We recommend removing this section entirely as consumers do not have the right to see, correct, access, obtain, delete, or port their personal data if the controller says it is not possible to identify them because the data is pseudonymous. The ability to move data in and out of different categories, which are subject to different rules, makes tracking and controlling personal data more difficult for consumers. Controllers could justify hiding the data it has about consumers by declaring that the data is pseudonymous, then process that data as identifiable data when convenient.

Section 11: Data Protection Assessments

Sec. 11(1) and (2) These subsections require controllers to conduct data protection assessments in certain circumstances such as when they process personal data for targeted advertising or to share personal data. But some of the situations in which assessments are required are very limited. For instance, assessments must be conducted when personal data is processed for profiling, but only "where such profiling presents a reasonably foreseeable risk" of things such as unfair or deceptive treatment of consumers, financial, physical or physical harm, intrusion on the private concerns of consumers, or other "substantial injury." Data protection assessments must also be conducted where there is processing of sensitive data and processing involves personal data that presents a "heightened risk of harm to consumers." It is up to the controller to make these determinations. There is no general requirement for controllers to assess their data practices.

Data protection assessments can help controllers understand what data they need and for what purposes, with the aim of minimizing the data they collect and only using it for the purposes that are necessary; what data needs to be disclosed to third parties and for what purposes, with the aim of minimizing that sharing; what analysis they need to conduct about the disparate impact that their data collection, use and sharing may have on different populations, with the aim of ensuring that their practices do not have unfairly discriminatory effects; whether the mechanisms

they have put in place to respond to consumers' questions, complaints, and requests to assert their rights are adequate; what controls they need to put in place to secure the data they hold and to ensure that third parties adequately secure it; and whether their practices align with their public privacy commitments and their legal obligations.

Recommendation: We recommend adding language requiring controllers to create Data Protection Assessments prior to all processing, setting the expectation that consideration of the key aspects of the processing, including the effect on consumers, is a routine part of their internal operations.

Sec. 11(1)(e) This provision creates a risk-benefit analysis for data protection assessments that leaves it to controllers to decide whether the benefits to them outweigh the rights of consumers.

Recommendation: We recommend removing language allowing for controllers to determine what constitutes a "heightened risk to consumers."

Sec. 11(3) This section allows the attorney general to request a data protection assessment that is relevant to an investigation it is conducting. But it makes clear that the assessment must be kept confidential, exempt from public scrutiny. These assessments shed light on the basis for companies' actions regarding consumers' personal data and the privacy policies they commit to.

Recommendation: We recommend removing the exemption from public inspection and making the data protection assessments available to the public.

Section 12: Limitations and Applicability

Sec. 12(1)(a) This provision seems to state that this statute does not supersede or preempt any existing regulation. A data trafficker could avoid compliance by finding an existing statute that arguably covers the same ground, and arguing that that statute controls. It also appears to directly contradict Section 22, which states that this statute preempts local rules and laws.

Recommendation: We recommend removing this section and Section 22.

Sec. 12(1)(b) Terms such as "investigation" or "regulatory inquiry" are not defined, and it is unclear what specific legal procedure would apply. There have been many concerning instances where law enforcement agencies have demanded that companies turn over consumers' personal data without any formal legal process.

Recommendation: We recommend defining these terms and making clear what specific legal procedure would apply.

Sec 12(1)(c) This provision allows for controllers or processors to warrantlessly share data with law enforcement. If data is subject to requisition by law enforcement, people should have the opportunity to consent to that possibility in advance.

Recommendation: We recommend adding a requirement for a warrant for controllers or processors to share data with law enforcement.

Sec. 12(1)(h) This provision does not have a consent requirement for use of data for research. Without a consent requirement, controllers are able to use or sell consumers' data for research based solely on its own risk-benefit analysis. For example, with the current language, a direct-to-consumer genetic testing service would be able to use consumers' genetic information for scientific research that enhances its own offering to consumers as long as it has some benefit to society, without the knowledge and consent of those consumers.

Recommendation: We recommend adding language requiring that controllers ask consumers for affirmative, non-ambiguous, and informed opt-in consent in order to use their personal data for research.

Sec. 12(2)(b) This provision allows controllers and processors to collect, use, or retain data to "perform solely internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller…" This language is vague, and it is unclear what would be considered "reasonably aligned with the expectations of the consumer."

Recommendation: We recommend removing this phrase and specifying the concrete types of internal operations that would allow controllers and processors to collect, use, or retain data. We also recommend making clear that personal data shall be deleted after a consumer concludes their relationship with the controller or processor.

Sec. 12(4) This provision removes responsibility from controllers and processors that disclose personal data to a third-party controller or processor if they "did not have actual knowledge that the recipient intended to commit a violation." The requirement to prove that controllers or processors had "actual knowledge" that the recipient of the data intended to commit a violation is a near impossible burden of proof to meet. Controllers and processors should be held responsible for what third parties do with consumers' data.

Recommendation: We recommend that this provision be removed.

Section 12(5)(a) This provision states that obligations imposed on controllers and processors under this chapter shall not adversely affect the rights and freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment of the United States Constitution. This provision is concerning because controllers and processors are considered persons. Because this bill affects their freedom to collect, use, and share data, controllers and processors could argue that they are exempt from the entirety of this bill.

*Recommendatio*n: We recommend removing this provision entirely as it is unclear what concern this provision is meant to address, or at a minimum, modifying this provision to read that the obligations imposed may not "unconstitutionally limit the rights or freedoms of any natural persons."

Section 13: Annual Registration Requirement

This section requires controllers and processors to register with and provide information to a newly created Washington State Consumer Data Privacy Commission.

Sec 13(1)(b)(iv) and (v) Controllers and processors are required to report "the amount of personal data collected, process, or shared" of both Washington consumers and globally in the preceding year.

Recommendation: We recommend modifying this language to read: "A statement specifying the amount of personal data collected and the number of consumers from which personal data are collected, processed, or shared globally in the preceding year; A statement specifying the amount of personal data of Washington consumers collected and the number of Washington consumers from which personal data are collected are collected, processed, or shared in the preceding year."

Section 14: Washington State Consumer Data Privacy Commission

The creation of a new funded data privacy commission is a meaningful improvement from SB 5062.

Sec 14(2)(f) and (g) These provisions preclude, for a period of one year after leaving office, individuals from accepting employment with a controller or processor that was subject to an enforcement action or civil action under this chapter during the member's tenure, or during the five-year period preceding the member's appointment. Additionally, individuals are precluded for a period of two years after leaving office, from acting, for compensation, as an agent or attorney for, or otherwise representing, any other person in a matter pending before the commission if the purpose is to influence an action of the commission.

Recommendation: To strengthen the above provisions, we recommend lengthening both the one-year period and the two-year waiting period to five years. Doing so will mitigate undue influence upon the Commission caused by movement of Commissioners from acting in a public service capacitive to lobbying activities. We also recommend removing the word "compensation" to prevent individuals acting to influence an action of the commission with or without compensation.

Section 15: Rule-Making Authority of the Washington State Consumer Data Privacy Commission

This section gives the Washington State Consumer Data Privacy Commission rule-making authority.

Section 16: Duties of the Washington State Consumer Data Privacy Commission

Sec. 16(11) This provision mandates that the Commission perform data protection audits on request, but it is not clear how the Commission would recoup those costs. Funds are often

generated only *after* successful enforcement action shave already been taken and it may be difficult to project with certainty how much will be available.

Recommendation: We recommend requiring the state to provide funds for enforcement, in order to create a stable and predictable budget for that purpose. Funds from enforcement actions could be used for purposes such as consumer and business education.

Section 17: Powers of the Washington State Consumer Data Privacy Commission

This section gives the Commission power to order a controller or processor to provide any information it requires for the performance of its duties and allows the Commission to subpoena witnesses, compel their attendance, administer oaths, take testimony of any person under oath, and require by subpoena the production of any items material to the performance of its duties or exercise of its powers.

Section 18: Administrative Enforcement

Sec. 18(1) This provision gives the Commission the discretion to decide not to investigate consumer complaints or decide to provide a controller or processor with a time period to cure the alleged violation. It allows the Commission to consider: "lack of intent to violate this chapter" and voluntary efforts by the controller or processor to cure the alleged violation prior to being notified by the commission of the complaint. It is unclear how the Commission would determine that there was "lack of intent to violate" privacy protections and an easy standard for controllers and processors to meet. Furthermore, there should be no requirement for the Commission to consider a "cure." There is no definition of or guidance as to what would constitute a cure. Ultimately, as with any enforcement agency, it should be left to the Commission to decide whether a company's practices merit investigation or any other type of action.

Recommendation: We recommend that this vague language and the reference to a cure be removed.

Sec. 18(4) This provision directs the Commission to hold a hearing to determine if a violation has occurred when it has determined there is reason to believe that this chapter or a rule adopted by the Commission has been violated. If the Commission determines that a violation has occurred, the Commission is required to issue an order requiring the violator to do all or any of the following: cease and desist the violation; or pay an administrative fine of up to $2,500 for each violation or up to $7,500 for each intentional violation and each violation involving the personal data of a minor.

Recommendation: Because it would be very challenging to prove that a violation was intentional, we recommend creating one standard maximum administrative fine, and increasing that fine to $25,000 per violation (or more) or up to four percent of annual revenue of the covered entity, controller, processor, or third party, whichever is greater. This number is much smaller than the EU General Data Protection Regulation's (GDPR) maximum fine of €20 million (roughly $20 million) or 4% of worldwide turnover for the preceding financial year.

Sec. 18(5) This provision allows for the Attorney General to request a stay of administrative action or investigation so that the Attorney General's Office may proceed with an investigation or civil action. The Commission may not pursue an administrative action or investigation unless the Attorney General subsequently determines not to pursue an investigation or civil action.

This provision and Sec. 19(6), which prevents the Attorney General from pursuing an action after the Commission has issued a decision, makes it so that the best course of action would be for the Attorney General to request a stay of administrative action or investigation for many cases. Consumers may find it difficult to understand which entity has ultimate authority to connect an investigation and issue decisions.

Recommendation: A Commission action should not preempt the Attorney General from acting. We recommend that the investigative process should be streamlined and clarified through consultation with the Attorney General's Office.

Section 19: Enforcement by the Attorney General

Sec. 19 Giving the Attorney General the power to enforce under the Consumer Privacy Act is an important inclusion in this section.

Recommendation: To strengthen this section, we recommend including the following language: "In an action brought by the Attorney General, the court may award: (1) injunctive relief, including preliminary injunctions, to prevent further violations of and compel compliance with this chapter; (2) civil penalties of up to $25,000 per violation or up to four percent of annual revenue of the covered entity, controller, processor, or third party, whichever is greater; (3) other appropriate relief, including restitution, to redress harms to individuals or to mitigate all substantial risk of harm; and (4) any other relief the court determines appropriate. When calculating damages and civil penalties, the court shall consider the number of affected individuals, the severity of the violation, and the precautions taken to prevent a violation."

Sec. (19)(4) This provision prevents the Attorney General from filing a legal complaint against a controller or processor without first sending a warning letter identifying the alleged violation of the law and giving the business 30 days to cure the violation. This provision sunsets on July 31, 2023. This "right to cure" provision would allow companies to violate the law and people's privacy rights without facing any accountability. After initiating and conducting a resource-intensive investigation, the Attorney General's Office would be required to use more resources to provide violators with an opportunity and tools to correct any violations. It should be up to the Attorney General's Office to decide when taking formal legal action is the appropriate measure and it should not be the right of the violator to avoid any accountability even when the Attorney General has determined that taking formal legal action is in the public interest. Furthermore, the lack of formal action would prevent legal precedents from being set, injunctive relief from being obtained, compensation for consumers from being ordered, court-approved settlements from being reached, and penalties from being assessed for practices that may have harmed large numbers of consumers or particularly vulnerable populations.

Recommendation: While the right to cure is not permanent, given the significant concerns of this provision, we recommend removing it entirely.

Sec. (19)(6) This provision prevents the Attorney General from filing an action under this section for any violation after the Commission has issued a decision against a controller or processor, even if that decision is to not investigate the violation.

Recommendation: We recommend removing this provision as Commission action should not preempt the Attorney General from acting. As discussed above, we recommend working with the Attorney General's Office to streamline and clarify the administrative enforcement process and the interplay between the Commission and the Attorney General.

Section 20: Private Right of Action

This section creates a private right of action and allows individuals to recover "actual damages" which is important but does not state that there is a minimum per violation penalty and attorney's fees. Although "actual damages" can be recovered, in practice, substantial actual damages can be virtually impossible to prove. Additionally, without coverage of attorney's fees, individuals would be required to invest money in a private right of action, posing a high barrier to entry. Lastly, this provision includes a 30 day right to cure.

Recommendation: To ensure that this private right of action is strong and meaningful, we recommend removing the right to cure and including the following language: "Any individual alleging a violation of this chapter or a regulation adopted under this chapter may bring a civil action in any court of competent jurisdiction. An individual protected by this chapter my not be required, as a condition of service or otherwise, to accept mandatory arbitration of a claim under this chapter. A violation of this chapter or a regulation adopted under this chapter with respect to the captured personal information of an individual constitutes a rebuttable presumption of harm to that individual. In a civil action in which the plaintiff prevails, the court may award: (1) liquidated damages of $10,000 per violation or actual damages, whichever is greater; (2) punitive damages; and (3) any other relief, including but not limited to an injunction, that the court determines appropriate. In addition to any relief awarded, the court shall award reasonable attorneys' fees and costs to the prevailing plaintiff.

Section 21: Consumer Privacy Account

Moneys in this account may only be used for the purposes of recovery of costs and attorney's fees accrued by the Attorney General in enforcing this bill and for the Commission.

Section 22: Preemption

This section preempts location jurisdictions from passing stronger privacy laws. For example, this section prohibits jurisdictions in Washington from passing broadband privacy laws that require internet providers to obtain people's opt-in consent before selling their data. It would also prevent, for example, the passage of local privacy laws protecting workers.

Recommendation: We recommend removing this section as local jurisdictions should be allowed to enact stronger privacy protections.

Section 23: A new section is added to chapter 42.56 RCW to read as follows

"Data protection assessments submitted by a controller to the attorney general in accordance with requirements under section 11 of this act are exempt from disclosure under this chapter."

Recommendation: As discussed above, we recommend removing this section as data protection assessments should be made transparent and available to the public.

Section 24: Data Collection Fee on Data Controllers and Data Processors

This section imposes an annual fee upon every data controller or data processor that is required to register with the commission beginning on or after January 1, 2023. The fee is to be assessed by the Commission sharing with the department of revenue a complete directory of all data controllers and processors registered with the Commission. All fees must be deposited into the consumer privacy account and may be used only for the operating expenses of the Commission.

Section 25

Sections 1 through 22, 24, and 26 of this act constitute a new chapter in Title 19 RCW.

Section 26

Sections 1 through 24 of this act take effect July 31, 2022.

Section 27

This section exempts institutions of higher education until July 31, 2027.

Recommendation: We recommend removing this provision. The act should be applicable to all entities at the same time.

Section 28

This section exempts nonprofit corporations until July 31, 2027.

Recommendation: We recommend removing this provision. The act should be applicable to all entities at the same time.

Section 29

This section includes a severance provision.

September 30, 2020

ACLU-WA Feedback on Washington Privacy Act Draft – 2021

Part 1

Section 101: Definitions

- **"Consent"** – With this definition, consent could be satisfied by a person simply clicking through a long and obscure privacy notice that they did not read.
- **"Consumer"** – This definition should include individuals a covered entity knows or has reason to know are located in Washington State—not just residents.
- **"Deidentified data"**- A key problem is that this definition is that it relies on compliance on the data controllers themselves. Public commitments and contracts mean very little without actual enforcement, which consumers cannot do under this bill. Which means that the concept of deidentified data as used in this bill is essentially a large loophole removing massive amounts of data to a lower tier of protection, essentially at the controller's election—and that controller can simply change their mind down the line to bring that trove of data back to the identifiable category.
- **"Personal data"** – This definition is defined much too narrowly. It should not exclude de-identified data or publicly available information. Personal data should capture any information that could be linked directly or indirectly to a person, household, or device.
- **"Pseudonymous data"** As with the deidentified data definition in this bill, this definition constitutes a big loophole. Separate storage is an ineffective means of protecting data. Companies would have the discretion to change data categories at their will. A meaningful privacy bill would allow consumers to retain power and clarity around which of their data is subject to what restrictions.
- **"Sale"** – The definition of "sale" raises many concerns. Sale is defined as the exchange of personal data for monetary or other valuable consideration by the controller to a third party. It explicitly exempts "the disclosure or transfer of personal data to an affiliate of the controller." This is concerning because it would be very difficult if not impossible for people to know which affiliates controllers are connected to, what the affiliates are, what the affiliates do. If affiliates of controllers would like to process people's data, they should be required to obtain opt-in consent. Additionally, this definition explicitly exempts "information that the consumer intentionally made available to the general public via a channel of mass media." This is concerning because consumers that share information publicly on social media are most likely not aware of if, how, for what purpose, for whom, and to whom that information is being sold or processed. Both of these exemptions should be removed.
- **"Sensitive data"** – This definition and category of data should be removed entirely from the bill, as all data can be "sensitive." Even ostensibly innocuous

data can be used to infer racial or ethnic origin, mental or physical health conditions, sexual orientation, or citizenship or immigration status. It does not make sense to have a separate category of "sensitive data" that is treated separately in this bill.

Section 102: Jurisdictional Scope

- This section should not exempt nonprofit corporations, institutions of higher education (especially as many institutions of higher education are for-profit institutions), and personal data covered by some federal laws. There is no reason to exempt personal data when federal laws do not prevent states from providing stronger protections.

Section 103: Consumer Rights

- This section lacks the right for people to know with which third parties controllers are sharing their data. This makes it difficult if not impossible for people to access, correct, delete, transmit, and consent to their data being processed because they would not know what third parties (e.g., data brokers) are using their data.
- 103(2) – Correction: This subsection gives controllers broad basis to deny a person's request to correct their data. The language, "…taking into account the nature of the personal data and the purposes of the processing of the personal data" is unclear. Such language would make it difficult for people to understand when they have the right to have their data corrected and makes it easy for controllers to deny the right to correction.
- 103(5) – Opt out of certain processing: People should have the right to opt-in, not merely to opt out.

Section 104: Exercising Consumer Rights

- The problem with including protections only for "known child[ren]" in the Washington Privacy Act is that companies may think the best practice is to avoid gaining actual knowledge in the first place. This leads to the unfortunate situation where businesses are collecting personal information from children by claiming not to know whose information is being collected rather than taking reasonable steps to give notice and obtain parental consent.

Section 105: Responding to Requests

- 105(3)(d) - If a controller fails to put an "authentication" mechanism in place when they collect people's data, they should not be able to use that fact avoid complying with people's privacy rights.
- 105(4)(a) – This paragraph states that controllers must establish an internal process whereby consumers may appeal a refusal by the controller to fulfill a person's data privacy rights. This process has no third party visibility or outside engagement. It would allow a large and powerful company to create barriers for people trying to exercise their rights.

- 105(4)(d) – A written explanation of why a person has been denied their data rights does not provide sufficient transparency and accountability.

Section 107 – Responsibilities of Controllers

- 107(1)(b) – Again, people should not just be able to opt-out, affirmative opt-in consent should be given for data processing to occur for any purpose.
- 107(5) – Controllers should establish data security practices tied to industry standards or stronger standards.
- 107(7) – Opt-in consent should be given for any data processing to occur—loyalty programs included. Currently, the language allows controllers to sell personal data to third parties without consent if the sale is "reasonably necessary to enable the third part to provide a benefit to which the consumer is entitled."
- 107(9) – The language "terms of service" should be added here given that there may be no contract or agreement in many cases.

Section 108 – Processing Deidentified Data or Pseudonymous Data

- This section suffers from the overbroad definitions of deidentified and pseudonymous data. The broad definitions would allow controllers to move data in and out of different categories (which are subject to different rules), making tracking and control over these data more difficult for people. This section also rests on a false sense of security about these data categories, which receive little meaningful protection. This entire section and accompanying definitions should be removed.

Section 109 – Data Protection Assessments

- 109(1)(e) – The controller would be the one determining what constitutes a "heightened risk to consumers," not the consumers themselves. This language should be removed. All data processing should be included in these assessments.
- 109(2) – Controllers would be determining the "benefits" and costs here. Given that this is a self-policing mechanism with no immediate outside accountability, it seems likely that benefits will be overstated and costs understated.
- 109(3) – Making DPAs exempt from public disclosure undercuts transparency and accountability. The data protection assessments mandated by this section should be made publicly available.

Section 110 – Limitations and Applicability

- 110(1)(a) – This seems to state that this statute does not supersede or preempt any existing regulation. A data trafficker could avoid compliance by finding an existing statute that arguably covers the same ground, and arguing that that statute controls. It also appears to directly contradict Section 114, which states that this statute preempts local rules and laws.
- 110(1)(b) - The terms "regulatory inquiry" and "investigation" are not defined and it is unclear what specific legal procedure would apply. The paragraph as a whole is far too broad. Controllers should fight for the rights of their customers, as has happened

in the case of companies resisting and litigating government efforts to request confidential consumer data.

- 110(1)(c)- If data is subject to requisition by law enforcement, people should have the opportunity to consent to that possibility in advance.
- 110(1)(h) – There is no consent requirement for use of data for research. This should be added.
- 110(2)(a) – The "internal research" exemption should be removed. This exception allows controllers to hold on to all consumer data indefinitely whether or not people request their data to be deleted. This language prioritizes controller's business interests over people's privacy rights.
- 110(2)(c)- The language "reasonably aligned with the expectations of the consumer" is vague. Consent should be sought for any processing of data. Additionally this paragraph should not allow data to be processed for internal operations after the consumer concludes their relationship with the controller.
- 110(4) – The requirement to prove that controllers had "actual knowledge" that the recipient of the data intended to commit a violation effectively immunizes controllers for providing data to third parties. How often will a controller have the actual knowledge of an intent to commit a violation? This section should be removed.
- 110(5)(a) – This paragraph presents a huge loophole. Presumably, controllers and processors are persons, and this bill will impact their freedom to traffic data. This arguably renders the entire bill meaningless.
- 110(7) – How does the controller "bear the burden" and in what process? Because the enforcement mechanism is limited, it is unclear what this language accomplishes.

Section 111 – Liability

- This section prohibits a private right of action. People need a private right of action to hold companies accountable for privacy violations and incentivize those companies to respect people's rights. Without strong enforcement, the bill is an ineffective vehicle for individual consumers to be able to enforce their rights. All that will be enforceable are large, systematic patterns of violations, while individual consumers will still be dependent on the generous spirit of data controllers, who in effect will have all the power in the equation.

Section 112 – Enforcement

- The "right to cure" language should be removed.
- The Attorney General's Office has previously requested that this section include injunctive relief and the ability of the court to award the agency reasonable costs and attorneys' fees, including investigative and expert costs.

Section 114 – Preemption

- Local jurisdictions should be able to enact stronger privacy protections and should not be preempted by this law.

Section 115 – Attorney General Report

- This section requires that the Attorney General's Office compile a report evaluating the liability and enforcement provisions in the bill and provide recommendations regarding the efficacy of these provisions. The Attorney General's Office has already provided feedback on the limitations of this bill and the flaws with the exemptions in Section 104. It does not seem that such a report would be necessary. It would be more effective to implement the recommendations already provided by the AGO.

Section 117

- Data protection assessments should be made publicly available.

Part 2

This section should be removed from the data privacy bill and treated separately. We recommend reviewing a contact tracing confidentiality bill that recently passed in New York: https://www.nysenate.gov/legislation/bills/2019/s8450

We also recommend reading a blog from Electronic Frontier Foundation that compares two approaches taken with federal public health privacy bills, and names the Public Health Emergency Act (PHEPA) as a good start. https://www.eff.org/deeplinks/2020/05/two-federal-covid-19-privacy-bills-good-start-and-misstep

Finally, we strongly recommend consulting ACLU's white paper describing governance principles for tech-assisted contact tracing. We encourage using the principles described in this paper to inform any data privacy legislation specific to public health emergencies. https://www.aclu.org/other/aclu-white-paper-government-safeguards-tech-assisted-contact-tracing

General comments

- Almost all of comments in Part 1 apply to Part 2.
- Part 2 lacks a private right of action.
- The right to cure language should be removed.
- The definition of emergency health data should be at least as expansive as the definition in the PHEPA.
- The preemption clause should be removed.
- A bill regarding data privacy in a public health emergency should also cover manual contact tracing.
- Part 2 should require opt-in affirmative consent for processing of any data, including deidentified data.
- If a person requests data to be deleted, processing should stop immediately and that data should be destroyed.
- The bill should require data to be deleted after it is deemed no longer useful for the specific purpose it was collected.