February 9, 2021

RE: Analysis of Concerns about the Washington Privacy Act, S. 5062

From: Susan Grant, Director of Consumer Protection and Privacy
Consumer Federation of America

One of the primary concerns about the Washington Privacy Act, S. 5062, is that is it based on the outdated "notice and opt-out" framework that fails to provide consumers with meaningful control over their personal information. It places the burden on them to understand what's going to happen with their data – a tall order in today's complex data ecosystem – and take steps to avoid unwanted uses, instead of placing the responsibility on businesses to seek their consent for specific data uses. Where the default lies matters, as marketers well-know. It's time to change the default to "opt-in."

The Washington Privacy Act also fails to provide adequate privacy protections. For example:

- It gives consumers *no* rights concerning the personal data that may be gleaned from social media and other "channels of mass media" if they didn't adequately restrict access to that information.
- It gives consumers *no* control over businesses selling their personal information to affiliated companies.
- It requires opt-in for processing consumers' "sensitive data" but not for *uses* of their personal information that may be sensitive.
- It allows consumers to opt-out of *seeing* targeted advertising based on tracking their activities over time on multiple websites and apps and profiling them, but that opt-out does not *stop* the tracking and profiling from occurring.
- It does *not* apply to advertising based on tracking consumer's activities over time on the company's own website or app and profiling them – the business model of Google and Facebook, which profit from profiling and targeting consumers on behalf of other businesses.
- It *only* gives consumers the right to opt-out of profiling when it is used "in furtherance to decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer." There is no overall right to *stop* being tracked and profiled.
- It does not apply to consumers' personal information when it is in the hands of financial services companies or other businesses that are covered by other laws, *even if the privacy protections of those laws are much weaker*.
- It limits consumers' rights to see the data that has been collected about them to the personal information they *provided* to the business; they have no right to see the information the business has obtained about them from other sources or gleaned through tracking them.
- It allows parents and legal guardians to exercise consumer's rights but does *not* enable consumers to designate others to act on their behalf, as California's privacy law does.
- It lets controllers and processors off the hook if the third parties to which they disclosed consumers' data violate the law if they *didn't know those parties intended to violate the law*.
- It *prevents* consumers from taking legal action to enforce their rights.
- It creates a "right to cure" that *hampers* the attorney general's ability to take action to stop bad practices and obtain remedies for consumers. California eliminated this from its privacy law.

A detailed analysis of these and other shortcomings of this bill follows. This does not include Part 2 of the bill. Addressing the public health emergency should be done separately. New York has already acted and that law could serve as a model. See https://legislation.nysenate.gov/pdf/bills/2019/S8450C. For questions contact Susan Grant at sgrant@consumerfed.org.

Section 101 Definitions

(6) This definition uses the passive voice to describe "consent" (page 4, starting on line 25) as a "freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data related to the consumer for a narrowly defined particular purpose."

Why does this matter? There are only a few situations in which processing consumers' data requires their permission under this bill – for instance, to process "sensitive" information about them. The current language does not make clear that consumers must take *action* to agree. The term "express affirmative consent" is often used in law when it is important to ensure that the consumers decided to agree to something. This definition would be stronger if it said: *"Consent" means that the consumer freely provides express, affirmative agreement 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.* The prohibition against the use of "dark patterns" in this definition (line 32) is crucial to protect consumers from inappropriate manipulation in order to obtain their consent.

(23) (a) The definition of personal data (page 6, starting on line 6) is not broad enough to encompass current and future data practices. Modern definitions of personal data use the phrase, "could be linked or reasonably linkable to an individual, household or device."

Why does this matter? Devices such as computers, cell phones, "smart" appliances and vehicles can produce data about the physical movements and locations of users, the times of those movements, whether there is someone in a household with a particular health condition, and other very revealing information that can be used advertising and other purposes without the need to ever identify individuals by name. Personal information must be defined, as recommended above, to reflect this.

(28) This allows for the use of pseudonymous data, which is personal data that can't be attributed to a specific person without the use of additional information, as long as that additional information is kept separately and subject to technical or organizational measures to ensure that the personal data is not attributed to an identified or identifiable person (page 6, starting on line 28).

Why does this matter? Pseudonymous data is not necessary since data that cannot be used to identify the consumer is already covered in the definition of deidentified data. Data would no longer be deidentified if information was added to it that would allow the consumer to be identified. There is no reason to carve out a separate category of data that is essentially not considered personal data for purposes the statute and that creates a separate risk that must be ameliorated by restrictive measures. This definition and the references to it elsewhere should be eliminated.

(29) (b) (iii) Companies' exchanging consumers' personal data with affiliates in return for money or some other form of valuable consideration is exempt from being considered a "sale" (page 7, starting on line 2).

Why does this matter? Companies are increasingly merging with and buying other companies, which in many cases are in completely different lines of business. Consumers have no idea who these affiliates are or what they do. Whether affiliates are subject to the parent company's privacy policies is an internal decision, not a legal requirement. From a consumer's perspective, it is how personal information is going to be *used* that is important, not whether it is going to be used by a related or unrelated company. This exemption would deny consumers the same ability to prevent their data from being sold to affiliates that they have for sales of their data to unrelated businesses.

(29) (b) (iv) (A) and (B) The exemption from the definition of "sale" 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 also highly problematic (page 7, starting on line 4). Arguably, this would include information from consumers' use of social media. Furthermore, **(iv)** does not describe this information as "personal data," in contrast to the rest of **(28) (b)**.

Why does this matter? This exemption would deny consumers the ability to prevent their personal information harvested from sources such as social media from being sold. The fact that consumers' personal information may be gleaned from social media does not mean that they *anticipated* that it would be sold, nor does their failure to restrict their data to specific audiences mean that they *intended* it to be sold. Furthermore, because of the wording used in **(iv)**, it appears that this data would not be considered "personal information" for purposes of the rights and obligations under the bill, such as the right to ask the controller to delete the data and the controller's obligation to keep the data secure.

(30) The definition and category of sensitive personal data do not provide the privacy from inappropriate data practices that one might think (page 7, starting on line 10). Personal information may be *used* in ways that are sensitive, even if the information itself is not. For instance, Target determined that when women bought seemingly innocuous items in combination, such as cotton balls and unscented lotion, they were likely to be pregnant – and not only pregnant, but in their third trimester. The company then used that information to target ads for certain baby products.

Why does this matter? While the bill requires controllers to obtain consumers' consent to process sensitive data, consent is not required to process data that do not fall into the sensitive category but the *use* of which may be sensitive. Later provisions in the bill prohibiting controllers from processing personal data on the basis of certain factors for certain purposes (page 16, starting on line 16) do not squarely address this problem. This is an illustration of why it is so important to require consent for any use of consumers' personal information for purposes beyond fulfilling their requests.

(33) (a) The definition of targeted advertising (page 7, starting on line 25) excludes advertising that is based on tracking consumer's activities over time on the controller's own website or using its app. This is precisely the business model of businesses such as Google and Facebook, which profit from profiling consumers based on their activities on their sites and using their apps over time to serve them targeted ads on behalf of other businesses. Furthermore, targeted advertising is defined as *displaying* ads based on tracking and profiling consumers; it does not include the *acts* of tracking and profiling themselves.

Why does this matter? The practical effect of this definition is that the consumer's right to opt-out of targeted advertising under **Section 103 (5)** does not apply to the advertising practices of Google and Facebook – a huge gap. Furthermore, because of the way targeted advertising is defined, consumers can opt-out of the ads being *displayed* to them but not out of being tracked and profiled. The personal

information compiled by this tracking and the profiles that are created based on it can be used for purposes other than advertising (including sharing with law enforcement). Moreover, this personal data is vulnerable to breaches no matter what it is used for.

(34) The definition of third parties excludes affiliates (page 7, starting on line 35). As previously explained, affiliates of companies should be treated the same way as unrelated companies.

Section 102 Jurisdiction

This section exempts from the law personal data that are covered by certain Washington state and federal laws. For example, **(2) (i)** (page 10, starting on line 1) exempts personal data collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA) which imposes some privacy obligations on financial service companies.

Why does this matter? Many of the laws cited here do not provide strong privacy protection and rights. For example, the only control GLBA provides consumers with regard to their personal information is the ability to opt-out of their data being disclosed to third parties (with a large loophole for joint business ventures). There are no rights with regard to targeted advertising, no rights to correct, port or delete one's data, and no protections from profiling or discriminatory use of one's data. There is no reason why Washingtonians should have *weaker* privacy rights with regard to their data when it is in the hands of one type of commercial entity versus another. Unless preempted, this bill should only exempt data covered by other laws to the extent that those laws provide *stronger* privacy protections.

Section 103 Consumer Rights

This section is the heart of the bill (page 10, starting on line 36). It is confusing, however, and contains subtle wording that unfairly limits the rights it purports to provide.

(1) gives consumers the right to confirm whether the controller is processing personal information about them and "access the categories of personal data" the controller is processing, but the subsequent rights in **(2)** and **(3)** to correct and delete one's data would be impossible to exercise by only being able to access the "categories" of data of the controller is processing.

Why does this matter? Consumers need to be able to *see the data* that the controller has about them in order to determine if corrections are needed and whether to delete the data.

This might be addressed by **(4)** which gives consumers the right to obtain the data the controller has about them, and in a portable form, except that this right is limited to the personal information "the consumer previously provided to the controller."

Why does this matter? The practical effect of this limitation is that consumers cannot access the data that the controller may have obtained about them from data brokers and other sources (this data "augmentation" is a common commercial practice. Furthermore, it is unclear whether consumers would have the right to access profiles that have been created about them from their activities, offline and online, as they did not necessarily "provide" that data to the controller.

Another issue is that the consumer's right to correct the data under **(2)** is qualified by "taking into account the nature of the personal data and the purposes of the processing of the personal data."

Why does this matter? It is left to the data controller to determine that qualification, and it is not clear on what basis the controller would do so. The practical effect is that consumers may find themselves unable to correct their data.

In **(5) (a)**, as previously noted, the right to opt-out of targeted advertising is limited by the definition of targeted advertising and the right to opt-out of the sale of one's data in **(5) (b)** does not apply to sharing with affiliates.

The right to opt-out of profiling in **(5) (c)** is limited to when profiling is used "in furtherance to decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer."

Why does this matter? The practical effect of this is that consumers do not have the right to choose not to be profiled and have assumptions made about them – assumptions which may not be accurate or fair, or which they simply would prefer not to be made – unless those assumptions would have some kind of legal or significant effect on them. Furthermore, it would be up to the controller to make that determination and allow them to opt-out of profiling or not. Consumers should have the right to avoid profiling, period. Furthermore, profiling should only be done if consumers opt-in.

Section 104 Exercising Consumer Rights

(2) In the case of processing the personal data concerning a "known child," the parent or legal guardian may exercise the consumer rights set forth in 103 on the child's behalf (page 11, starting on line 22).

Why does this matter? This wording 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 data were processed. If the consumer is a child, a parent or legal guardian should be able to exercise its rights, whether or not the controller knew the consumer was a child.

(3) This allows guardians, conservators, and others who have "protective arrangements" concerning consumers under state law to exercise the rights in **103** on their behalf (page 11, starting on line 25). It says nothing, however, about others whom consumers may authorize to act on their behalf.

Why does this matter? Consumers may ask for help managing their affairs from a relative, a friend, a volunteer at a senior center, a social worker, a health aide, someone at the Better Business Bureau or a state or local consumer protection agency, or someone from another type of service that provides consumer assistance. As California's privacy law provides, consumers should be able to designate agents to exercise their privacy rights on their behalf, and as long as reasonable verification is provided, the controller should honor the agents' requests.

Section 105 Responding to Requests

This section (page 11, starting on line 30) sets out requirements for controllers to establish internal mechanisms for responding to consumers' requests to exercise their rights and for handling their appeals if they are not satisfied. At the end of the day, however, the only recourse consumers have if they are not satisfied with the controller's response is to complain to the attorney general's office.

Why does this matter? This section highlights why it is so important for consumers to have a private right of action to enforce their rights. The attorney general's office may be able to resolve some of these disputes informally through mediation, but that does not create legal precedents, ensure that other

consumers in the same situation get their problems resolved, or require businesses to change their practices. Furthermore, the attorney general's office will never have the resources necessary to take formal legal action in every case that may merit it. When consumers believe that their rights have been violated, they deserve to be able to enforce them, not only to resolve their own problems but to reform business practices for the good of all.

Section 106 Responsibility According to Role

This important section (page 13, starting on line 26) on the responsibilities of controllers and processors contains wording that creates loopholes through those responsibilities could be evaded.

(2) (a) The responsibility of a processor to assist the controller in responding to consumers' requests to exercise their rights is qualified by the initial phrase, "Taking into account the nature of the processing..."

Why does this matter? It is not clear what this means or who makes the determination about the nature of the processing. It would be clearer and stronger to delete this phrase and simply begin by saying that the processor should assist the controller. There is already another qualification in the sentence, "insofar as this is possible." "Taking into account the nature of the processing" also appears in the beginning of **(2) (b)** concerning notice of data breaches. Again, that phrase should be deleted.

(4) A similar phrase, "Taking into account the context of processing," appears in describing the controller's and processor's responsibility to take appropriate measures to secure consumers' data. It is not clear who determines the context of the processing, but in any case this qualification is not necessary and should be removed.

Section 107 Responsibilities of Controllers

(1) This sets out the requirements for informing consumers about the controller's data practices and their rights in that regard (page 15, starting on line 26).

(1) (a) This calls for privacy policies to be "reasonably accessible, clear and meaningful." It should go further to require that they be conspicuous wherever consumers interact with the business, that they be in plain language and avoid legal jargon, that they be available in all languages in which the company interacts with consumers, and that they be formatted in a manner that makes them easy to follow.

Why does this matter? It is widely acknowledged that few consumers read privacy policies because it is too time-consuming and they are typically written in dense language full of legalese, making them difficult understand. If the required notices are intended to be truly useful to consumers, not just to lawyers, they must be formatted and worded in a manner that makes them as easy as possible for people to read and understand. The state office of privacy protection should be instructed to develop model privacy notices based on independent research, which is available from many academic institutions, and focus-group testing.

That agency should also be instructed to develop standardized wording for information that is 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. Again, this work should be informed by independent research and testing.

As noted before, controllers should only be able to sell consumers' data to third parties, use it for targeted advertising, or to profile them for purposes other those necessary to fulfill their requests by obtaining their express affirmative consent. **(1) (b)** would need to be revised to reflect this, and should have the same requirements as **(1) (a)** in terms of language and formatting. Again, the state office of privacy protection should be instructed to develop models to help businesses comply and ensure that consumers have the information they need to make these decisions.

(5) The provisions concerning security practices (page 16, starting on line 16) should require controllers to meet or exceed applicable industry standards.

Why does this matter? Industry security standards 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.

(7) This provides crucial protections for consumers from being discriminated against by denying them goods or services, charging them different amounts, or providing them with different levels of quality of goods and services if they exercise their rights under this law (page 16, starting on line 30). For example, it would prohibit businesses from charging consumers higher prices if they opt-out of seeing targeted ads displayed, or from offering consumers products or services at a lower price if they opt-in to their sensitive personal data being processed. It would not prohibit controllers from denying goods or services, charging different amounts, or providing different levels of qualify of goods or services to consumers who voluntarily participate in loyalty, rewards, premium features, discounts or club card programs. The term "voluntary participation" is too vague, however, and the disclosure requirements for processors are inadequate.

Why does this matter? These programs typically collect large amounts of data about the products and services that consumers purchase, how much they spend, and in the case travel-related programs, where they go. Voluntary participation could be construed to include negative option offers in which consumers are enrolled in the programs unless they cancel. Affirmative express consent should be required. Furthermore, in seeking to obtain such consent, controllers should be required to clearly explain what types of personal information will be used for the program and for what purposes, what types of information will be shared with third parties, and they will do with the information. Consumers should also be informed about the restrictions placed on those third parties. In addition, controllers should be required to delete consumers' personal information when they cancel participation in the program and to instruct third parties with which it has been shared to do so.

(8) In prohibiting the processing of "sensitive data" without the consumer's consent, or in the case of a child, the parent's or guardian's consent, the term "known" child is again problematic (page 17, starting on line 9). The Children's Online Privacy Protection Act (COPPA) which is referred to here and the rules under it apply to "any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child." Furthermore, COPPA only applies to websites and online services.

Why does this matter? 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.

(9) The important protection here from any attempt to limit or waive consumers' privacy rights in a contract or agreement (page 17, starting on line 15) should include "the terms of service."

Why does this matter? In many interactions between consumers and businesses there is no "contract" or "agreement" per se, but there are terms of service, which are unilateral and typically buried on the website, that may contain important terms governing the rights and obligations of the parties. Adding "terms of service" would make clear that any limits or waivers of consumers' privacy rights there are unenforceable.

Section 108 Processing Deidentified Data or Pseudonymous Data

(2) Consumers do not have the right to see, correct or delete their personal data if the controller says it is not possible to identify them because the data is pseudonymous (page 17, starting on line 19).

Why does this matter? Combined with the limited disclosure of categories of data in **103 (1)**, a controller could use **108 (2)** to justify hiding the data it has about consumers by declaring that the data is pseudonymous, and then return it to processing as completely identified data when convenient.

Section 109 Data Protection Assessments

(1) (a) – (e) This requires controllers to conduct data protection assessments in certain circumstances (page 18, starting on line 15) such as when they process personal data for targeted advertising or sale 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 when sensitive data is processed or it 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.

Why does this matter? 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. Controllers should be required 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.

(2) This 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 (page 18, starting on line 37).

Why does this matter? This is very different than the General Data Protection Regulation (GDPR) in Europe, to which this bill is sometimes compared. In the GDPR, consumers' privacy rights are paramount and if they outweigh commercial interests, there is no legal basis for the data processing.

(3) This allows the attorney general to request a data protection assessment that is relevant to an investigation it is conducting (page 19, starting on line 9). But it makes clear that the assessment must be kept confidential, exempt from public scrutiny.

Why does this matter? These assessments shed light on the basis for companies' actions with regard to consumers' personal data and the privacy policies they commit to. They should be available to the public.

Section 110 Limitations and Applicability

(1) (a) and (b) (page 19, starting on line 28) allows controllers and processors to comply with other federal, state or local laws and demands for consumers' personal data from governmental authorities, despite the restrictions and consumer rights under this law. While some terms such as "subpoena" and "summons" are straightforward and refer to court-approved requests, others such as "investigation" or "regulatory inquiry" are vague, and no notice is required to be provided to consumers.

Why does this matter? There are many instances in which concerns have been raised about law enforcement agencies demanding that companies turn over consumers' personal information without any formal legal process. **(c)** is also concerning, because consumers should have notice and an opportunity to consent or object to the cooperation envisioned here except in certain circumstances that should be carefully delineated.

(1) (h) (page 20, starting on line 15) allows consumers' personal data to be used for research in the public interest if it is likely to provide substantial benefits that do not exclusively accrue to the controller, the benefits outweigh the privacy risks, and the controller takes steps to mitigate those risks. It does not require the data to be deidentified or that consumers must provide consent for the research.

Why does this matter? It cannot be left to the controller to use or sell consumers' personal data for research based solely on its own risk-benefit analysis. This would enable a direct-to-consumer genetic testing service, for instance, to use customers' genetic information for scientific research that enhances its own offerings to consumers as long as it has some overall benefit to society, without the knowledge and consent of those customers. Consumers must be informed and asked for express affirmative consent in order to use their personal information for research.

(2) (b) (page 20, starting on line 28) provides that the obligations of controllers and processors under the law do not restrict their ability to perform "solely internal operations that are reasonably aligned with the expectations of the consumer based on consumer's existing relationship with the controller…"

Why does this matter? It is not clear what would be considered "reasonably aligned with the consumer's expectations." Any provisions that essentially excuse controllers and processors from the limitations and obligations under this law must be narrowly and carefully tailored. Providing examples of the types of internal operations that would be allowed here would be helpful.

(4) This provision (page 21, starting on line 8) lets a data controller or processor off the hook when a third party to which it discloses a consumer's personal information violates the law if it "did not have actual knowledge that the recipient intended to commit a violation."

Why does this matter? This completely removes any responsibility on the part of the data controller or processor to monitor the actions of those third parties to ensure that they are living up to their contractual obligations in regard that data, since a showing of actual knowledge of someone else's intent is an impossible burden of proof to meet. The incident in which Facebook sold consumers' personal information to Cambridge Analytica, which used it for purposes that Facebook did not authorize and that consumers would never have expected or agreed to, is a good example of why controllers and processors must be held responsible for what third parties do with consumers' data.

(5) (a) (page 21, starting on line 19) provides that the obligations imposed on controllers and processors shall not "adversely affect the right and freedoms of any persons, such as exercising the right to free speech…" It is not clear who the "persons" are here – the controllers and processors, or the consumers – and what concern this is meant to address.

Why does this matter? Provisions that may narrow the obligations under the law must be clear and justifiable. Otherwise, they can create loopholes that can be exploited to escape responsibility.

Section 111 Private Right of Action

(1) This provides that violations of this law may not serve as a basis for a private right of action "under this chapter or under any other law" (page 22, starting on line 8). It further states in **(2)** that the rights consumers had before July 1, 2020 under Washington's unfair commercial practices law, the state constitution, the U.S. constitution, and other laws are not altered.

Why does this matter? This prevents consumers from taking legal action against companies that violate this law or from asserting that violations of this law constitute violations of other laws under which they have private rights of action, essentially slamming the courthouse doors in their faces. There is no justification for this. It is the job of judges to decide whether lawsuits have merit and to dismiss frivolous lawsuits. It is not up to legislators to decide that consumers' lawsuits are unjustified and prohibit them. The ability to seek justice is a fundamental American value. The idea what consumers have no power to hold businesses accountable, while businesses can and do sue consumers every day to enforce their contacts, intellectual property rights, and other interests, is patently unfair.

Section 112 Enforcement

(4) This provision (page 22, starting on line 29) 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.

Why does this matter? This greatly hampers the ability of the attorney general to enforce the law and obtain redress for consumers. There is nothing to prevent the attorney general's office currently from

sending a letter to a business or arranging a meeting to discuss concerns about particular practices, and this is often done in mediating individual consumer complaints informally. It is up to the agency, however, to decide when taking formal legal action is the appropriate measure; it should not be the right of the business to automatically forestall such action when the agency has concluded that it is in the public interest. What constitutes a "cure" is not defined, but even if the controller or processor resolves the matter voluntarily, 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 governing businesses' future conduct, and penalties from being assessed for practices that may have harmed large numbers of consumers or particularly vulnerable populations. It would also prevent the attorney general from recouping the costs of investigations. Notably, the right to cure, which first surfaced in the California Consumer Privacy Act, has been eliminated in the ballot measure recently approved by voters.

Section 114 Preemption

This preempts local privacy protections that were enacted on or after July 1, 2020 (page 23, starting on line 19).

Why does this matter? While this leaves in place consumer protections such as the Seattle broadband privacy rule, which was enacted before that date, it blocks new privacy protections at the local level – protections that are not in this bill but that local authorities may see as vital in the future. Preemption is only appropriate to the extent that this law provides stronger privacy protection than local laws, and local authorities should have the ability to enforce it.

Section 117

This allows requires data protection assessments submitted to the attorney general to be kept in secret (page 24, starting at line 9). As noted earlier, this is information that should be accessible by the public.