Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

Writers email: eellman@cdiaonline.org
Writer's direct dial: +1 (202) 408-7407
CDIAONLINE.ORG

April 23, 2020

Mr. William McGeveran
Reporter, ULC Collection and Use of Personally Identifiable Data Committee
Mondale Hall
229 19th Ave., South
Minneapolis, MN 55455

Via Email: mcgeveran@umn.edu

Dear Mr. McGeveran:

This letter supplements and incorporates by reference CDIA's comment submitted on April 14, 2020 to the Collection and Use of Personally Identifiable Data Committee ("Committee") on the Collection and Use of Personally Identifiable Data Act ("Draft Act"). While this comment primarily addresses issues that CDIA did not address the April 14 comment, this comment also amplifies a few selected points raised in that April 14 comment.

As you know, the Consumer Data Industry Association (CDIA) is the voice of the consumer reporting industry, representing consumer reporting agencies, including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA's comment on April 14 and this comment will help the Committee create a privacy model bill that is workable for all stakeholders: consumers, businesses, governments, and nonprofits.

1. Application of the Draft Act

A. The definition of "personal data" should exclude aggregated data

The Draft Act exempts deidentified data from the definition of "personal data," but there is no express exemption for aggregated data, or data that is associated with a group of data subjects where individual data subject identities have been removed. The CCPA incorporates such an express exemption, and we urge the Committee to similarly include this exemption.

B. Clarify the deidentification process

The Draft Act exempts deidentified data from its scope, or data where the capacity to identify or otherwise link the data with a particular data subject "has been eliminated." Considering the fact that there may continue to exist ways to reidentify data, even if such methods are difficult to accomplish or unlikely to occur, we urge the Committee to add the word "reasonably" before "eliminated" to require deidentification efforts that are reasonable in light of the particular circumstances.

C. Define "biometric and genetic data"

The Draft Act defines "biometric and genetic data" as a component of "sensitive data" but does not define "biometric and genetic data." The Committee should define "biometric and genetic data." The CCPA defines "biometric information" as an individual's physiological, biological, or behavioral characteristics, which could be a starting point for the Committee.

D. The employment exemption should be expanded to better serve workers

The Draft Act exempts "[p]ersonal data collected or retained by an employer with regard to its employees that is directly related to the employment relationship," § 3(b)(6). In CDIA's April 14 comment, I noted that the employment exemption should be expanded to cover agents, contractors, owners, directors, managers, and other non-employee workers. The Committee should also focus less on personal data and more on data. I now want to offer a proposed change to benefit these workers and their principals during and after their work. The Committee can protect consumers and recognize the modern workforce by exempting "data collected, used, or maintained in an employer-employee relationship, an employer-applicant relationship, a principal-agent relationship, or other work relationship."

E. The fraud exception should be expanded

The fraud exception, contained at § 3(c)(2), is broad and covers most potential fraud, loss, and security incidents, but it could be improved by adding

> <u>(vi) corruption, money laundering, and export controls; and (vii) protection against, prevent, detect, investigate, report on, prosecute, or remediate actual or potential corruption, money laundering, export controls</u>."

Adding these issues to the list would bring § 3(c)(2) into consistency with § 3(c)(4).

F. The Draft Act should be limited to data subjects in consumer relationships

The Draft Act appears to apply to not just consumer transactions, but also to business to business transactions. The unnecessarily broad scope of the bill is found in § 3(a) where the "Act applies to the commercial activities of a person who conducts business [in 20 the State of X] or produces products or provides services targeted to [the State of X…" CDIA believes the Committee should narrow the proper focus of the Draft Act to apply only to consumer transactions. The best way to focus on consumers is through a definition of a consumer and limiting the Draft Act's application to consumer transactions. Both the senate and house versions of the Washington privacy bills set a good example for the Committee to follow. The Washington bills defined a "consumer" as a "natural person who is a Washington resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context." Wash. S.B. 5376 (2020), § 3(6) and H.B. 1854 (2020), § 3(6).

G. Provisions on devices should be removed from a consumer protection act

Since privacy laws should protect consumers, not devices, CDIA respectfully requests that the Committee remove references to devices in the Draft Act. In addition to device protection being out of place in a consumer protection law, it will be difficult at best for companies to give data subjects access to their own device data.

2. **The rights of data subject rights needs a different approach**

Section 4's data subject rights do not, on their own, make it clear how a controller complies with the rights. In particular, the right to correction, § 4(3), includes no guidelines by which a controller would be expected to extend this right in accordance with the Draft Act. The right to deletion, § 4(4), needs to incorporate exceptions from this right, similar to those included in the CCPA, beyond those provided for in § 3. Without fleshing out these rights, it will be impossible for a controller to comply with the expectations of the Draft Act.

Additionally, § 5, relating to a data subject's right to a copy of their personal data, needs to be fleshed out to include guardrails on how a consumer makes such a request. The right needs to have reasonable limits, like limiting the disclosure to information the controller collected within the last 12 months, since a consumer has the right to make such a request for free every 12 months. Similarly, § 6 needs clarity on what constitutes a sufficient opt-in for this section.

Section 7(a) permits a data subject to exercise any rights under § 4 "by any reasonable means" while § 7(d) permits controllers to adopt procedures for data subjects to use to exercise their rights. We request the Committee to clarify this provision by amending § 7(a) as:

A data subject may exercise rights under section 4 of this act by notifying the controller by way of the methods specified by the controller as required under section (d) of this Section and Section 8 of this [act] ~~by any reasonable means~~ of the data subject's intent to exercise one or more of these rights.

Similarly, any appeal right should be set by the controller's procedures, so § 7(d)'s language on appeals should be removed.

Finally, § 7(b) requires a controller to comply with a consumer's request within 45 days or a reasonable time. We urge the Committee to consider providing for an express extension period for good cause, such as an additional 45 days.

3. **Filing a data privacy commitment with States is unmanageable**

Section 8(a) requires controllers to file with a state Attorney General or other designated agency a data privacy commitment with detailed content about the controller's privacy practices. The volume of such commitments would be very high and, as a result, likely unmanageable for a state Attorney General, who is usually tasked with enforcing laws and not administrative tasks. Section 8(b) requires the commitment to be provided on a controller's website, and such public disclosure should be sufficient and the most likely source for consumers seeking information about how to exercise their rights.

4. **Creation of "duties" is unnecessary and adds to business risk without any consumer benefit**

The Draft Act creates many duties on custodians, like a duty of loyalty, Draft Act § 9; a duty data security, *id.*, § 10; a duty of data minimization, *id.*, § 11; a duty of transparency, *id.*, § 12; and a duty of purpose limitation. Establishment and use of duties create unnecessary liability without creating any new benefits. The Committee can easily rephrase the captions to "enforcement," "data security," "data minimization," "transparency," and "purpose limitation."

5. **Data processor agreements need greater flexibility**

Section 14 requires data processing by a processor to be governed by a written contract with certain specified contract. However, the required contract is excessive in relation to the need for appropriate and needed contractual controls on the data. CDIA urges the Committee to consider the CCPA language for service provider agreements.

6. Data privacy assessments need flexibility

Section 16 requires controllers and processors to conduct data privacy assessments for all data processing activities, but the required content of the assessments is overly prescriptive and does not permit sufficient flexibility depending on the nature of the processing, the nature of the data, and the entity's previous assessments. CDIA urges the Committee to consider flexibility in these requirements, such as how the proposed Washington Privacy Act dealt with data processing assessments.

7. Enforcement of the Draft Act needs clarification

Section 9, the duty of loyalty, prohibits engaging in processing activities that are unfair, deceptive, or abusive acts or practices. However, states already have UDAP or deceptive trade practices laws, and the Draft Act should not demand uniformity out of differing state UDAP regimes.

Otherwise, § 9 is duplicative of § 19 and therefore can be eliminated. Sections 19 and 20 need adjustment as well, particularly with regard to private rights of action. CDIA believes that an appropriate compromise might be to permit private rights of action but only for continued violations following Attorney General enforcement, as § 20(b)(3) and (4) propose. Section 20(b)(2) is particularly problematic because it would incentivize controllers to use soft and noncommittal language in its privacy commitment and would be difficult and costly to litigate.

8. The Committee should remove the "opt-in" provision from Section 6

A state mandated opt-in highly controversial and unprecedented and those reasons allow could threaten enactability of the Draft Act. Since the Draft Act already provides for notice, deletion, and opt-out rights, the inclusion of a specific opt-in, even for sensitive personal data, is not necessary and would create challenges and confusion both for consumers and for businesses regarding the legitimate use of sensitive personal data.

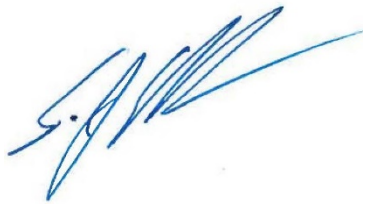
9. The data privacy assessments required by Section 16 goes too far

The Draft Act exceeds even that which is required by the CCPA, the failed Washington Privacy Act ("WPA"), and the General Data Protection Regulation ("GDPR"). This section is overly prescriptive and onerous. CDIA asks the Committee to delete or revise this Section to a general, flexible requirement that is appropriately tailored for the types of data at issue, the activities of the business, and similar actions. CDIA also requests that the Committee remove the retention requirement and regulatory oversight provisions since these are already amply covered by existing statutes, rules, judicial decisions, or private agreements.

Conclusion

Thank you for the opportunity to serve as an observer to the Committee's work and to comment on the Draft Act. We appreciate the time and effort that has gone into an attempt at a model privacy bill to serve all stakeholders. Our comments improve a promising project in ways that recognize legal and commercial realities to serve consumers, businesses, nonprofits, and government agencies. Please let me know if you have any questions or need additional information.

Sincerely,



Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs