CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

May 5, 2020

VIA ELECTRONIC FILING

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

RE: April Revision of Model Draft for Collection and Use of Personally Identifiable Data Act ("Draft Act")

Dear Mr. McGeveran:

The U.S. Chamber of Commerce ("the Chamber") respectfully submits these supplemental comments to the Uniform Law Commission ("ULC" or "Commission") regarding the Draft Act concerning the collection and use of personally identifiable data. The Chamber agrees that uniformity should be the ultimate goal with regard to privacy policy, and for this reason believes that only a national privacy law is properly suited to provide protections to all Americans equally. The Chamber reserves the right to further supplement these comments and is soliciting input from member companies on issues regarding health data, portability, sectoral treatment, service provider issues, and location data.

I. SCOPE

A. Legitimate Uses of Data

The Chamber recommends that the Commission eliminate from the mandated privacy requirements the legitimate uses of data highlighted in the Chamber's model privacy legislation such as those meant to protect security, fight fraud and money laundering, debug errors affecting functionality, support of network management, and research.

Additionally, the Commission should confirm the definition of targeted advertising to reflect established practices in the U.S. and the European Union. Applying a privacy choice to the use of data collected over time and across unaffiliated websites and apps for targeted advertising is consistent with the European Union's GDPR, which permits such activity provided there is an appropriate legal basis for it (usually interpreted as legitimate interest or consent) and allows individuals to opt out of such uses. Targeted advertising is also permitted in the United States on an opt-out basis, per the FTC's 2012 privacy framework and the California Consumer Privacy Act (CCPA). For the past decade, the Digital Advertising Alliance has provided an opt-out mechanism under an online behavioral advertising self-regulatory framework supported by the Federal Trade Commission as a privacy-protecting mechanism for consumers to address such targeted advertising. The Draft Act should permit use of personal data on an opt-out basis

consistent with these global best practices for targeted advertising across websites and apps. The general need to justify any data processing under the Draft Act in order to ensure its legitimacy should not be so expansive that it prevents such routine uses as targeted advertising and supporting business operations.

Lastly, businesses may use data to personalize one's experience with targeted promotions in the same website customers are using so that they can see relevant products and services. These practices do not involve sharing or selling data to a third party The Draft Act should permit the same short-term transient uses without being subject to a blanket opt-out right for targeted advertising.

B. 50 Percent Revenue Threshold

The Draft Act also imposes obligations on any person who "earns more than [50] percent of its gross annual revenue directly from its activities as a controller or processor of personal data." This criteria is extremely ambiguous, given that every company in America uses personal data in some way to deliver its products and services to consumers, to improve these products and services, or to provide services to another business. In order to ensure that the Draft Act's requirements are more targeted, its application should be limited to disclosure or sharing of data—not earning revenue "directly".

Activities as a controller or processor include accepting electronic payments. Because most payments controllers and processors accept are electronic payments, rather than cash, many more businesses will be subject to the Draft Act's obligations than likely anticipated by the drafters of the threshold, including a majority of consumer-facing businesses and many other businesses that accept electronic payments. That is true, for example, of many of the smallest, single store-front businesses in the nation. Such a threshold therefore undercuts the idea that the law should not burden small businesses, which is why a rule tying legal obligations to earning a majority of revenue from the sale of data is a more reasonable and practicable threshold for achieving the Draft Act's intended goals.

C. Governments

Many high-profile events such as the OPM data breach have highlighted how data can be exposed in the hands of governmental entities. The Chamber argues that the requirements of the Draft Act should also extend to state and local governments, many of whom are requesting that companies turn over the very personal information to be protected by the Draft Act. Without governmental obligations, if a private citizen wanted to sue because the government misused privately obtained personal data, the liability stops with the company that may have been forced to share data as a cost of doing business in a particular region.

II. DATA SUBJECTS RIGHTS

The Chamber agrees that consumers should have clearly defined rights. For example, consumers should have the right to know how data is collected, used, and shared; be able to delete data; and opt out of sharing. At the same time, the Draft Act fails to impose a verified request standard that many other states like California have either adopted or are considering. Companies should not be required to honor unverified requests or to collect, retain or combine additional information in order to fulfill data subject rights.

The Draft Act also fails to establish a secure, private and streamlined intake process so that businesses can keep track of data subjects' rights requests. Section 7(a) of the Draft Act permits "notifying the controller *by any reasonable means* of the data subject's intent to exercise one or more of these rights." This could lead consumers to attempt to exercise rights requests in public and in communications with temporary or untrained employees that have no access to corporate systems handling personal data to log those requests and permit the business to act on them. Businesses should be given the flexibility to establish the most secure channels through which consumers may make rights requests so that businesses can verify their receipt and act on them. Additionally, the right to correct inaccuracies should be limited to correction of inaccuracies that materially affect the consumer, and there should be an extension of time, similar to the GDPR and CCPA, permitting businesses a total of 90 days to make corrections and/or deletions.

III. DATA SUBJECTS RIGHT TO A COPY OF DATA

States already impose limitations on how many requests a consumer can make in order to obtain a copy of personal information. The Chamber's Model Privacy Legislation would allow consumers to obtain similar data once annually. Regulated entities should also be able to reject all abusive and excessive requests regardless of timeframe. The Chamber recommends that this provision apply to categories of information if the provision of the full copy of data would be overly burdensome. The requirement to give consumers a copy of data should be scoped only to personal data and not all data. Additionally, the Draft Act should not require that inferences from data be required to be transmitted to consumers as this information is not necessarily personal and could also be proprietary information. The requirement to enable the data subject to transmit the data to another data controller by automated means is confusing and impracticable because automated means is not defined, and this requirement should not apply to businesses where the business does not have the capacity to provide a copy by automated means or the data subject's requested copying would require transmission between businesses in unrelated lines of business or sectors where no common automated transmission process exists.

IV. DATA SECURITY

Data security standards should be limited to certain subsets of sensitive data, consistent with existing state data security and breach notification laws. All fifty states and four federal jurisdictions, including the District of Columbia, have data breach laws that require notification

for the disclosure of unencrypted sensitive data that would lead to a risk of significant harm, like identity theft. Many businesses have already implemented controls to ensure the security of this data from unauthorized use, and the Draft Act's proposed application of data security standards to cover all personal data, including non-sensitive data that would not lead to consumer financial harm if disclosed, would cost far more to implement than any consumer benefit it may provide.

Sincerely,

Jordan Crenshaw
Executive Director and Policy Counsel
Policy

Matthew J. Eggers
Vice President, Cybersecurity