CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

April 23, 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's ("the Chamber") and the U.S. Chamber of Commerce's Institute for Legal Reform ("ILR") respectfully submit these comments to the Uniform Law Commission ("ULC" or "Commission") in regards to 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.

Absent a national law, any model privacy bill, including a model state privacy bill, should promote uniformity and certainty. A privacy law should grant individuals clearly defined privacy rights. Additionally, uniformity also can only be achieved when enforcement mechanisms exist that promote certainty like attorney general enforcement, and not frameworks that promote uncertainty like inclusion of a private right of action. The Chamber objects to a process that includes private rights of action.

In 2012, the Federal Trade Commission codified the privacy framework that it has enforced for over 20 years.[1] This framework, including its definitions and risk-based approach, forms the foundation for the privacy programs of Chamber members and the basis for discussions of federal privacy legislation, as well as privacy bills at the state level for the past few years. The Draft Act neglects to adopt most of the basic definitions and concepts in this framework, however, which creates confusion

Individual privacy is paramount and a robust, consistent, balanced and uniform data framework will enable consumer protection and enable innovation to thrive. It is for this reason

[1] U.S. Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change (March 2012).

the Chamber has contributed ideas to developing uniformity by adopting its own model privacy legislation.[2] The Chamber offers the following recommendations regarding the Draft Act.

I. DEFINITIONS

A. "Deidentified"

The Chamber agrees with excluding deidentified data from the definition of "personal data" and recommends that the ULC should follow guidance provided by the Federal Trade Commission with regard to deidentification of data. Under the Commission's Draft Act, in order for data to be considered "deidentified", among things a custodian must have "[b]usiness processes that reasonably prevent inadvertent release of deidentified data." It is unclear how this requirement in the Draft Act would determine reasonableness as well as what harm the Commission is trying to prevent if data is deidentified. This novel definition of "deidentified data" is so broad that it is has to potential to make it nearly impossible to determine if data is deidentified.

B. "Personal Data"

The definition of "personal data" should be limited to "identifies…"—not "describes"—"…a particular individual…" The use of "describes" is an unprecedented expansion without clear meaning and could potentially apply to massive data sets including such things as the color shirt someone typically wears – in other words, data not traditionally understood to be personally identifiable information. As written, "describes" is not a precise definition. The business community suggests the phrase "using a reasonable amount of effort" is not very helpful due to its vagueness and more the drafters should provide more specificity as to what constitutes a "reasonable amount of effort."

The Commission should also strike the second sentence beginning with "Probabilistic inferences," which are typically proprietary observations or assumptions made by companies analyzing personal data and are not personal data itself. The European General Data Protection Regulation ("GDPR") does not count observations as personal data. The inclusion of "probabilistic inferences" is another significant expansion of the term "personal data" as traditionally understood in global privacy laws that should be eliminated from this definition.

The Commission should eliminate the new provision as well that includes household and device data. Such definitions and overly broad and unnecessary as the definition of "personal data" is meant to capture that identifies a particular individual.

---

[2] U.S. Chamber of Commerce Model Privacy Bill (Revised June 2018) *available at* https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf.

C. "Profiling"

The Chamber holds that the ULC should strike this definition entirely. The definition of "profiling" is overly broad and would cover necessary processing to complete a transaction (like a credit card purchase), or to ensure the safety and security of transactions or customers in their interactions with businesses. It sweeps in the ordinary practice of knowing a customer's preferred products, which poses little risk to consumers. All of these should be exempted and not just search queries, as called out in the second sentence.

The language relative to profiling and automated decision-making should specifically *exclude* insurance underwriting and rating. The inclusion of "physical location", "movements", "behavior" in the definition of "profiling" is particularly problematic when a company works to determine risk. Many of these uses of data in fact benefit consumers.

D. "Publicly available data"

The definition of "public available data" in Section 2 is too narrow especially the last phrase "provided the information is being used in a manner consistent with any conditions on its use imposed by law." This approach goes against the long-standing practice of federal and state Freedom of Information Act ("FOIA") laws and is likely to violate the First Amendment. If information is lawfully made available to the public and subsequently lawfully obtained by a third party, there should not be a restriction of a third party's use of such information. We support striking this definition and incorporating something more like the scoping definition in Section 3 that includes information "widely distributed in media."

E. "Sensitive Data"

The Chamber asserts that policymakers should base data protections on the risk that data presents to individuals. For example, social security numbers and account information if obtained by nefarious actors could pose real material risks to consumers. At the same time, defining types of data as sensitive in a manner that is overly broad could have negative unintended consequences for individuals.

For example, limitations on the use of characteristics such as race, ethnicity and gender in the current definition of "sensitive data" should be related to prevent invidious discrimination and limitations beyond this may have negative unintended consequences for customers and viewers. Personal data about race, gender, and ethnicity is used to promote inclusivity. For example, race and ethnicity are widely used audience demographics in the United States, and that while discrimination (including price discrimination) should be prohibited, it should be permissible to characterize audience segments by race and ethnicity. This kind if data is also used to ensure that customers receive products and services related to their race, ethnicity, or gender such as promotions regarding men's and women's clothing or traditional cuisines enjoyed by certain cultures. If sensitive data requires affirmative consent, then a significant amount of

marketing of such products and food would be curtailed and consumers may not be alerted to promotional pricing or coupons they want as a result.

One other point is that the Draft Act seeks to define "biometric" and "genetic" data as sensitive but does not define these terms. The Commission should draft a model law that provides clearly defined terms for these types of data.

F. Sign

The Chamber suggests striking this definition as unnecessary as discussed below. The Draft Act only uses this term once with regard to a designated officer signing a document. The Chamber finds no precedent for this term being defined in any major privacy laws or proposals.

II. SCOPE

A. Basic Threshold Requirements

i. 50,000 Individuals, Households, or Device

Any privacy legislation should consider disproportionate effects on small businesses. The Draft Act places a disproportionate burden on these companies. For example, the Draft Act mirrors the California Consumer Privacy Act in that it would cover business that handle the data of over 50,000 individuals, households, or devices. According to the State's own Regulatory Impact Assessment ("RIA"), the proposed CCPA Regulations will cost up to **$55 billion** in compliance costs for California companies alone.[3] The RIA estimates fail to account for lost revenue for companies, compliance with CPRA (if adopted), and integration of other state frameworks with CCPA. These costs will impose a significant burden on businesses.

CCPA applies to any company that does business in California and that "[a]lone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares the personal information of 50,000 or more consumers, households, or devices."[4] A food truck operator that takes electronic payments for 137 unique customers per day or an online seller in Arizona that advertises to 137 unique devices per day could be subject to the requirements of the Act and its Regulations. The State's RIA assumes that the Regulation will require companies with fewer than 20 employees to incur up to $50,000 in compliance costs.[5]

---

[3] *See* Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, State of California Department of Justice and Office of the Attorney General at 11 (August 2019) *available at* http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

[4] CAL. CIV. CODE § 1798.140(c)(1)(B).

[5] *See* supra note 5.

Imposing such a low threshold on businesses to be covered with have a negative and disproportionate impact on small businesses, especially those that are seeking to recover from the COVID-10 Pandemic.

ii. 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 qualifier goes beyond the CCPA's requirement that a business must derive more than 50 percent of its revenue from the *sale* of data. Every company in America uses data in some way to improve its products and services for consumers. Such a broad requirement should be limited to disclosure or sharing of data—not earning revenue "directly".

B. Relationship to Other Federal Frameworks

The Chamber believes that state laws should respect federal privacy provisions already in place and work to prevent conflict with laws such as the Children's Online Privacy Protection Act, the Communications Assistance of Law Enforcement Act, the Driver Privacy Protection Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Telephone Consumer Protection Act, and federal privacy authority for airlines in the Federal Aviation Act. The Chamber continues to receive feedback about how these federal laws should interact with state laws.

C. Exemptions for Legitimate Data Uses

i. Completion of a Transaction

The Draft Act states the "nothing in this act shall prevent the collection, authentication, maintenance, retention, disclosure, sale processing, communication, or use of personal information to (1) complete a transaction in goods or services that the data subject requested." This exception for the collection, use and dissemination of personal data to "complete a transaction in goods or services that the data subject requested" must be expanded to cover post-transaction processes expected by the consumer, such as the processing of data to ensure shipment, warranty coverage and other services related to the transaction. Businesses should be allowed to use data in a manner that improves and enhances products, services, and user experiences.

ii. Publicly Available Data

In addition to the comments above about the definition of publicly available data, "publicly available data" that is readily available on the Internet or in other traditional First-Amendment protected media should not be regulated under the Draft Act.

iii. Independent Measurement

Independent measurement is an important legitimate use of data. For example during the COVID-19 Pandemic inventory analysis for supply-chain purposes has been critical. Companies should be able to engage in research and measurement where the data is protected through appropriate security measures.

iv. Commercial and Employment Data

The Draft Act should not treat commercial data as "personal data." For example, information about commercial credit reporting, employees, job performance, independent contractors, job applicants and business-to-business ("B2B") contacts should not be subject to the requirements of this model legislation. With respect to the employee carve-out, it should also include information generated by employees in the course of performing their job as well as emergency contact info and beneficiary info provided by the employee within the context of the employment relationship. The CCPA exemption extends to both emergency contact and beneficiary information. Additionally, data about individuals unrelated to their capacity as consumers, such as shareholder information, should not be treated as personal data

v. Legal Claims

The Draft Act also enables companies to use and disclose data in a way that allows them to "comply with or defend claims under federal, state, or local laws, regulations, rules, guidance or recommendations…" The Chamber asserts this exemption include activities preparing for and asserting legal claims.

vi. Other Legitimate Purposes.

The Chamber recommends that the Commission eliminate from legal obligation the legitimate routine uses of data highlight in its model privacy legislation such as those meant to protect security, fight fraud and money laundering, debug errors affecting functionality, otherwise maintain and improve products and services, and network management.

D. 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 also extend to state and local governments, many of whom are requesting that companies turn over the very personal information to be protect 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.

III. 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. Additionally, the right to correct inaccuracies should be limited to correction of inaccuracies that affect the consumer.

In addition, though the Data Privacy Commitment would include a Data Custodian's preferred methods to receive data subject requests, there is also a statement that data subjects should be able to make requests by "any reasonable method." The Commission should delete the "any reasonable method" provision so that it is not read to require a business to respond to a request made by whatever means necessary. Companies should not be required to honor unverified requests and should be given the flexibility to establish the channels through which consumers may make rights requests, which will encourage enhanced security and certainty.

IV. 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.

V. DATA PRIVACY COMMITMENT

The Chamber recommends that the Commission strike Section 8 of the Draft Act pertaining to Data Privacy Commitments, which would require a company to file potentially 50 different copies of the commitments and take feedback from many different Attorneys General, many of which may not have the resources or expertise to evaluate companies' operational capabilities reflected in the Data privacy Commitment. Violating the Data Privacy Commitment would also give rise to a private right of action, so eliminating it would eliminate one predicate for this remedy. A more streamlined approach to consumer transparency would be to require companies to post a conspicuous privacy policy instead, and allow the Attorney General of a state to investigate and enforce against companies that do not comply with their stated policies.

VI. CUSTODIAN'S DUTY OF LOYALTY

The purpose of model privacy legislation is to instill certainty and uniformity. The Chamber supports a national privacy standard because data crosses states lines and business models are dependent on the analysis of data. Unfortunately, Draft Act's Duty of Loyalty defeats uniformity by enabling state Attorneys General (AGs) to define unfair, deceptive and abusive trade practices with no clear legislative guidance on what these acts would be. Moreover, this type of provision is novel and is not included in CCPA or GDPR. Such a framework would enable state AGs to define privacy violations with no clear, uniform standard. The ULC should strike the Duty of Loyalty as drafted.

VII. CUSTODIAN'S DUTY OF DATA SECURITY

Data security standards should be tailored to what is appropriate for the size and scope of the business, and the nature of the data uses. There should also be certain industry-recognized, globally accepted security standards a company could comply with to obtain a safe harbor, so that the Attorney General does not have unfettered discretion to determine what is reasonable security. The first sentence of Section 10 should reflect this principle. Additionally, security and data privacy risk assessments should be conducted separately. While generally aligned, many new and necessary security protections actually require the collection of more device information to discern users' normal and anomalous behaviors.

Ohio enacted an innovative cyber/data security law, the Ohio Data Protection Act (S.B. 220), in November 2018. S.B. 220 grants an affirmative defense against data breach tort claims to those businesses that bring their cybersecurity frameworks up to an industry standard. Other states' data protection laws tend to focus on requirements or penalties. The Ohio statute uses an affirmative defense to incentivize companies to improve their cyber practices. While the Chamber does not support the inclusion of a private right of action, the Draft Act should incorporate the affirmative defense provision of S.B. 220 as an affirmative defense to regulatory action.

VIII. CUSTODIAN'S DUTY OF DATA MINIMIZATION

The Chamber applauds the goal of the Commission to support the minimization of data. At the same time, the minimization should have exceptions for legitimate data uses. Without that exception, this provision shifts the balance of interests so far that it requires justification for many routine data uses that do not create a risk of harm for data subjects. This section should allow for the retention of data for the purposes unrelated to a transaction but that are necessary to prevent fraud or enhance security such as a transaction record. Other exemptions should be included such as enabling product recalls, warranties, or ongoing services that extend beyond an initial transaction or data used for law-enforcement request. The Draft Act should also permit companies to use data to maintain and improve their products and services.

IX. CONTROLLER'S DUTY OF PURPOSE LIMITATION

The Draft Act at Section 13 states that "[a] controller shall not process personal data, or permit processors or other persons to process personal data, for purposes that are not specified in the [privacy] notice to data subjects required by this [act]." In order for the obligations of this section to triggered, the purpose not specified should be *materially* different. The Draft Act should permit the use of data for a purpose that is compatible with the original purpose in the context of the original transaction without additional consent.

X. DESIGNATION OF DATA PRIVACY OFFICER

Section 15 should require a company have at least one data privacy officer company-wide and not officers for each state. There should be an exception to this requirement for small businesses such as sole proprietorships. The Draft Act should also eliminate the signature requirement for reach data privacy assessment required by the Act. The Draft Act should avoid imposing standards, duties and qualifications for a data privacy officer and should enable companies to have flexibility in determining who is qualified.

XI. DATA PRIVACY ASSESSMENT

The Chamber believes that accountability programs in businesses can be a valuable tool to ensure that consumers' privacy is respected. At the same time, the Draft Act proposes requirements that go beyond international norms and appears to require assessments for each processing activity an entity conducts. The Chamber would like to point the Commission in the Direction of Article 35 of the European GDPR that would focus these assessments on high-risk data processing.

The obligation to develop a *very detailed* privacy assessment, particularly for all processing activities, would be overly burdensome. The requirements to predict possible risks of harm may be challenging for some companies, particularly less sophisticated ones. The GDPR states that Data Protection Impact Assessments ("DPIAs") are to be completed prior to the commencement of applicable processing, which indicates that DPIAs are not required for processing activities in place prior to the GDPR's effective date. It is recommended that same type of language be added to the ULC document.

Regarding Section 16(a), the first part of the section requires assessments be revisited every two years. Undertaking 'update' assessments every two years simply based on a time period unnecessarily requires re-reviews of processing that has not changed and therefore poses no new risk. I recommend that the section be comprised of only the second sentence.

A ten-year retention requirement as provided for in the Draft Act seems unreasonable in situations where the assessments no longer align with the current processing. As aligned with

the GDPR's approach, the Chamber recommends the removal of a specific retention period or that the retention period be shortened substantially.

XII. Nondiscrimination

The Chamber recommends that Section 17 be struck in its entirety. The CCPA is instructive on this section as its similar requirements threaten consumer loyalty programs. CCPA prevents covered businesses from engaging in "discriminatory" practices such denying goods or services, charging different prices, or giving a different level of quality for collection, deletion, or sale of consumer data, or against consumers that exercise their privacy rights under the Act.[6] An overly broad interpretation of the Anti-Discrimination rights in CCPA threatens the ability of retailers, airlines, restaurants, and entertainment companies to offer loyalty and reward programs that greatly benefit consumers. According to one study, the overwhelming majority of consumers agree that loyalty programs save them money.[7] The Chamber strongly urges the Attorney General to interpret CCPA in a manner that ensures that the consumers continue to enjoy loyalty and rewards programs without disruption to businesses or their customers.

XIII. Regulatory Enforcement

The Chamber requests that companies be given the opportunity to cure privacy defects within 30 days after AG notification, particularly if an alleged violation is technical in nature and not willful or reckless.

XIV. Private Rights of Action

The U.S. Chamber and the U.S. Chamber Institute for Legal Reform (ILR) oppose private rights of action (PRAs) as a method of enforcing privacy laws, as they are particularly inefficient and ineffective in this policy area.

Privacy interests and harms can often be undeveloped or intangible in nature; but even in cases where privacy harms are arguably more concrete, it is often difficult or impossible to trace an alleged harm to a particular entity or defendant, or to a specific act or omission. Moreover, even when a consumer has suffered a concrete injury, they are unlikely to receive meaningful compensatory or injunctive relief through private litigation, especially when that litigation takes the form of a class action lawsuit.

Given these characteristics, attempting to enforce privacy laws through PRAs engenders a series of troubling consequences:

- PRAs allow individual plaintiffs' lawyers to set national policy. Rather, expert enforcement agencies such as the offices of the state attorneys general should

[6] CAL. CIV CODE § 1798.125(a).
[7] Emily Collins, "How Consumers Really Feel About Loyalty Programs," FORRESTER (May 8, 2017) *available at* http://www.oracle.com/us/solutions/consumers-loyalty-programs-3738548.pdf.

shape statewide policy with a more holistic approach. Agencies can be expected to understand the complexities of the law and to balance the various factors of encouraging compliance, supporting innovation, and preventing and remediating harm.

- PRAs lead to inconsistent and, potentially, to dramatically-varied rulings across jurisdictions. On the other hand, agency enforcement provides consistent decisions that shape privacy protections for consumers statewide, while also offering clarity to entities on how to align their practices with existing law.

- PRAs, combined with the class action mechanism, often lead to grossly expensive litigation and extreme pressure to settle as companies are faced with the alternative of significant reputational damage and the risk of an outsized (or "nuclear") verdict. This dynamic primarily benefits the plaintiffs' bar and offers little relief to consumers whose privacy interests they claim to represent.

No state has yet passed a comprehensive consumer privacy law that includes a private right of action for privacy violations. Consider the three states to have passed comprehensive privacy laws to date:

- Maine – Maine's Act to Protect the Privacy of Online Consumer Information (LD 946) does not include a PRA.[8]
- Nevada – Nevada's SB220 (Ch. 603A) does not include a PRA.[9]
- California – Even California did not see fit to extend PRAs to privacy violations. The California Consumer Privacy Act provides for PRA only in the context of security violations.[10]

In other states, such as Washington and New Jersey, the inclusion of PRA provisions led to the ultimate defeat of comprehensive legislation. It is difficult to understand, then, why a purported model bill would include an unprecedented broad PRA for privacy violations when no state legislature has seen fit to do so.

Stakeholders and CUPIDA Observers have clearly opposed the PRA provisions that appeared in the initial discussion draft. The majority of stakeholders who participated in the February 21-22 meeting on the CUPIDA discussion draft and weighed in on the PRA recommended its removal. It is therefore both concerning and unclear why the PRA provisions remain in the second draft. While the Chamber opposes the inclusion of a PRA in the Draft Act, it should not be the default position of the ULC to include a PRA and any such conversation about enforcement should be saved for after substantive obligations are determined.

[8] 35-A M.R.S. § 9301 (2019).
[9] Nev. Rev. Stat. § 603A (2019).
[10] Cal. Civ. Code. § 1798.100 (2018).

XV. Uniformity of Application and Construction

Section 21 of the Draft Act states that "[i]n applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that create it." The Chamber would assert that provisions in the Draft At such as the Duty of Loyalty and PRAs discourage uniformity. Additionally, the Chamber recommends that uniformity would be encouraged by taking the example of CCPA by preempting localities from imposing their own privacy requirements.

XVI. Effective Date

The Chamber recommends that the Draft Act mirror the GDPR and give companies two years to comply after promulgation.

Conclusion

The Chamber appreciates the opportunity to comment on the Draft Act, and is ready to work with the Uniform Law Commission in the future.

Sincerely,

Tom Quaadman
Executive Vice President
Chamber Technology Engagement Center

Harold Kim
President
U.S. Chamber Institute for Legal Reform

Matthew Eggers
Vice President
Cybersecurity Policy