June 24, 2020

To: **Harvey Perlman, Chair of the Collection and Use of Personally Identifiable Data Drafting Committee**

From: **Matt Starr, Centre for Information Policy Leadership (CIPL) and Observer on the Collection and Use of Personally Identifiable Data Drafting Committee**

Date: **June 24, 2020**

Re: **Inquiry on an Accountability and Risk-Based Approach to Privacy Legislation**

Dear Harvey:

I only recently became an Observer on the Collection and Use of Personally Identifiable Data Drafting Committee in early May, and thus was unable to provide feedback on the most recent draft prior to your April 24 meeting, so I appreciate the opportunity to provide input on the process now. The Centre for Information Policy Leadership (CIPL) is a global data privacy and security think tank in the law firm of Hunton Andrews Kurth LLP. Our mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. Our work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world.

First, we commend the Committee for including a risk-based approach to privacy regulation in its most recent draft of the Collection and Use of Personally Identifiable Data Act ("CUPIDA"). We have not seen the extent of this approach in other proposals put forth in the US thus far, which often rely heavily on notice and consent. It also does not rely on different "legal bases" for processing like the EU GDPR, which in practice still has too often resulted in an over-reliance on consent. Instead CUPIDA allows all processing unless it is unfair, discriminatory or abusive, as long as it is disclosed to the user, except in the cases of targeted advertising and profiling, where it requires opt-out or opt-in consent depending on the type of data being used. While we have flagged some specific concerns below and may not share this particular stance on targeted advertising and profiling, this approach is nevertheless broadly consistent with CIPL's message that the U.S. should adopt a risk-based approach to privacy law that does not place an outsized role on consent, and we offer below suggestions on how to improve upon the great work that the Committee has already done.

In response to your recent request for suggestions that address privacy legislation at a more fundamental level, I wanted to introduce you to some of the work that CIPL has done in this space. Our primary work stream has been educating stakeholders about the concept of organizational accountability[1] and the importance of including it in a comprehensive privacy law**.**

[1] See, for example, the following CIPL White Papers: The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, July 23, 2018, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; Incentivizing Accountability: How Data Protection Authorities and Lawmakers Can Encourage Accountability, July 23, 2018, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-

CUPIDA already captures some aspects of organizational accountability in its risk-based approach to privacy regulation, as well as its requirements relating to transparency and the designation of a data privacy officer. However we think a few additional changes could greatly improve the Act's ability to ensure that consumers are protected while promoting responsible use of data:

- The inclusion of a requirement for a comprehensive privacy program covering all core elements of accountability;
- Enabling formal accountability mechanisms like certifications and codes of conduct; and
- A risk-based approach to data usage, including for new purposes.

I will discuss each of these concepts briefly below, but all of them are explained in greater detail in CIPL's papers, several of which are cited in the footnotes. Additionally, I have included a brief discussion of why the inclusion of a private right of action would undercut the ULC's goal of uniformity.

Privacy Programs

Organizational accountability requires organizations to implement comprehensive privacy programs governing all aspects of collecting and using personal information. Such programs should address all core elements of accountability, as described further below. Accountability also requires that companies can verify and demonstrate the existence and effectiveness of such programs both internally and externally upon request, particularly to an enforcement body. Having a comprehensive privacy program in place enables compliance with applicable legal obligations, more effective protection for individuals and their data while also fostering trust and responsible data use, data sharing and cross-border data flows.

Accountability's essential elements include establishing leadership and oversight for data protection and the responsible use of data, including the appointment of a responsible person such as a data protection officer; assessing and mitigating risks to consumers; establishing internal policies and procedures around all aspects of data processing, including data security; providing transparency to all internal and external stakeholders; providing training for employees and raising awareness; monitoring and verifying the implementation and effectiveness of the privacy program and internal compliance; and implementing response and internal enforcement procedures, including complaint handling processes. A privacy program requirement in a privacy law should include all of those elements in some form. Indeed, this is what the Federal Trade Commission currently requires of companies, as evidenced by its privacy consent orders.[2] FTC Commissioner Christine Wilson praised CIPL's accountability framework in a recent speech

_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; Q&A on Organizational Accountability in Data Protection, July 3, 2019, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf; and What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework, May 2020, *available at* https://www.informationpolicycentre.com/organizational-accountability.html.

[2] For a further discussion of how the FTC's consent orders impose comprehensive privacy programs on organizations, please see CIPL's White Paper on Organizational Accountability in Light of FTC Consent Orders, November 13, 2019, *available at*

and urged companies to refer to it when building their privacy compliance programs, and state privacy laws should require companies to adopt such programs.[3]

As noted above, we appreciate that the most recent draft of CUPIDA already includes some elements of accountability, such as its requirements for data controllers and processors to designate a data privacy officer and conduct written data privacy assessments, but we think it could go further. Section 4 – Privacy Program and subsection 2 of Section 9 of the U.S. House Energy & Commerce Committee's staff draft privacy bill,[4] which was released last December, provide examples of how CIPL thinks a privacy program requirement should function in legislation. These sections could provide a model for CUPIDA, and we would be happy to work with you on the language.

Certifications and Codes of Conduct

In addition to requiring organizations to have comprehensive privacy compliance programs, any state privacy law should also enable formal accountability mechanisms such as privacy codes of conduct and certifications, particularly given the likelihood that different states will pass their own unique privacy laws. These mechanisms, if enabled by multiple states, could be made interoperable across different states through a variety of mechanisms or could each link to a common code or certification (modeled after, for example, the APEC Cross-Border Privacy Rules (CBPR)), which would allow for companies to comply with multiple state laws at once by adhering to a single set of privacy practices.[5]

In particular, these mechanisms can facilitate legal compliance and accountability for companies who use them. This benefits not only businesses, but also consumers and enforcement authorities. Consumers benefit through better privacy protections, transparency and accountability. Enforcement authorities, which may not have ample resources at the state level, may not have to devote as many resources to complaint-handling because much of the front-line complaint-handling could be part of the code of conduct or certification. Also, investigations of alleged violations will be more efficient where enforcement authorities can enforce against formally recognized codes of conduct or certification programs. SMEs, which often lack significant internal compliance staff and resources, will benefit from these external programs because they translate legal requirements into operational and scalable

---

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organizational_accountability_in_light_of_ftc_consent_orders__13_november_2019_.pdf.

[3] Keynote Remarks of Commissioner Christine S. Wilson at the Privacy + Security Academy, May 7, 2020, *available at* https://www.ftc.gov/system/files/documents/public_statements/1574938/wilson_-_remarks_at_privacy_security_academy_5-7-20.pdf.

[4] U.S. House of Representatives Committee on Energy and Commerce Bipartisan Staff Privacy Legislation Draft, Dec. 18, 2019, *available at* https://www.huntonprivacyblog.com/2019-12-18-privacy-bipartsian-staff-discussion-draft/.

[5] For more information on certifications and codes of conduct, please see the following CIPL White Papers: Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, April 12, 2017, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf; What Does the USMCA Mean for a US Federal Privacy Law?, January 17, 2020, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_what_does_the_usmca_mean_for_a_us_federal_privacy_law__01.17.2020__4_.pdf.

compliance steps and comprehensive privacy compliance programs. Certifications and codes of conduct also can serve as due diligence and risk-management tools for companies to identify and vet service providers, vendors and third-party processors. Additionally, they have many advantages relating to cross-border data transfers and global interoperability, which are further explained in our relevant materials.

We appreciate that the ULC is already trying to address the challenges that will result from each state developing its own unique privacy law through this process of developing a model state law. At the same time, formal accountability schemes such as codes of conduct and certifications are relevant even if they won't be used for interoperability and harmonization purposes, but simply as mechanisms to help organizations, particularly SMEs, have comprehensive accountability-based privacy programs in place. The Comments in CUPIDA's Data Privacy Commitment section already state that it is "envisioned as permitting the incorporation and use of voluntary consensus standards or best practices in compliance with this Act," and "that the incentive [for data controllers to publish how they intend to comply with the Act] is that following their own commitments provides a safe harbor for any private right of action." This sentiment is already in line with enabling formal accountability mechanisms, and thus this section could easily be expanded to include such an option.

Senator Wicker's recently proposed United States Consumer Data Privacy Act of 2019[6] provides an excellent example of how to incorporate certification language into a privacy law. It would give a regulatory body, in this case the FTC, the authority to approve third-party certification programs to create standards or codes of conduct for compliance with "1 or more provisions of this Act" including, and importantly, for entire privacy compliance programs. Any organization that is certified by an approved certification program would be deemed in compliance with the relevant provisions of the Act that are addressed by that program, subject to enforcement.

CIPL is also currently working on a white paper proposing the development of an interstate interoperability code of conduct/certification modeled on the CBPR system and incorporating substantive requirements from the currently prevailing US privacy standards, such as the CBPR, the EU-US Privacy Shield, the California Consumer Privacy Act and any additional substantive frameworks that may come on line in the near future. This code or certification, as mentioned, could serve as a bridging mechanism between different state laws, or as an accountability tool even if all states follow the same model law, or as a code or certification that might be enabled in a future federal privacy law.

Risk-Based Approach to Data Usage

As noted above, we would like to commend the ULC's decision to embrace a risk-based approach to privacy regulation in CUPIDA, as we believe such an approach maximizes both individual privacy protections and the effective use of data.[7] A data privacy assessment and balancing of interests in a way

[6] United States Consumer Data Privacy Act of 2019 Discussion Draft, Nov. 27, 2019, *available at* https://www.huntonprivacyblog.com/2019/12/03/senator-wicker-circulates-draft-privacy-bill/nc7/.

[7] For more information on risk assessments and a risk-based approach to privacy regulation, please see our white paper Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

that does not expose data subjects to an unreasonable material risk of harm demonstrates this risk-based approach. However, we think the risk-based approach could be expanded in CUPIDA to enable unexpected and additional uses of data that were not known or disclosed at the time of collecting the data but that pose little risk of harm to data subjects.

As it currently stands, CUPIDA's purpose limitation provision forbids processing of personal data for any purpose that is not specified to data subjects at the time their personal data is collected. We have concerns that this provision, as written, would restrict innovative uses of data that were not anticipated at the time of collection. This is particularly true with respect to rapidly developing AI technologies. Alternatively, it could result in expansive purpose specifications that do not benefit individuals. We would suggest, as an alternative, an approach modeled after the GDPR's legitimate interest balancing test to determine whether uses beyond what was initially disclosed to data subjects would be permitted.

The GDPR's legitimate interest basis for processing is a risk-based mechanism that allows for the processing of personal information where an organization's or a third party's legitimate interest in the processing is not outweighed by the interests or rights of the individual whose personal information is processed.[8] When an organization relies on this basis for processing, it must conduct a risk assessment to conduct a balancing test to assess whether their (or a third party's) legitimate interest is overridden by the "interests or fundamental rights and freedoms of the individual" (i.e., by the risks of harm to the individual). In effect, legitimate interest enables beneficial information uses, and ensures that future data uses that are currently not contemplated by a law may be enabled where they are not harmful. The importance of having such a mechanism in the law is highlighted by the current COVID-19 crisis where organizations around the world are suddenly confronted with the need to use data for public health purposes in ways not contemplated at the time of collection. Laws that do not enable such unforeseen but beneficial data uses will not only thwart effective responses to crises like the current one, but they will also undermine innovation and the digital economy and society more generally. Indeed, the Comment under Section 3 in the ULC's current draft bill acknowledges that the current draft does not yet address this particular issue.

The ULC should consider adopting a similar risk-based approach to allowing for secondary uses of data, particularly given that it already contains the parameters for a Data Privacy Assessment, which would be used to conduct the balancing test. Combined with a privacy program requirement and the other protections included in CUPIDA, such an approach would ensure that data subjects are not subjected to additional risk of harm from uses evaluated under the legitimate interest balancing test.

The American Law Institute's Data Privacy Principles[9] articulated a legitimate interest basis for secondary uses of data which may provide an example of how it could be incorporated into CUPIDA.

We would suggest that the Committee adopt a modified version of ALI's test, along the lines of "Secondary personal data activities may be conducted without consent if . . . the personal data activity serves a

[8] For more information the legitimate interest basis for processing, please see our white paper CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data, April 27, 2017, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_27_april_2017.pdf.

[9] Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text* (2019), *available at* https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3483257_code249137.pdf?abstractid=3457563&mirid=1.

significant legitimate interest, and does not pose a significant risk of material harm to the data subject or others." The ALI further states that "a significant risk may exist with a low likelihood of a high-magnitude injury or a high likelihood of a low-magnitude injury."

Private Right of Action

CIPL is concerned that including a private right of action in a model state bill would undermine the ULC's goal of uniformity. Private rights of action create unpredictability and, through litigation and subsequent court decisions, would result in the same law being interpreted and enforced differently in each state. More centralized enforcement by AGs would reduce such divergence in interpreting and applying the law. We think that the Committee should not include a private right of action in CUPIDA and instead focus on provisions, such as those recommended above, that require businesses to implement a wide range of accountability measures designed to prevent harms to individuals. A certification mechanism, for example, could significantly augment AGs' enforcement by incorporating complaint handling requirements for companies and providing for third-party dispute resolution mechanisms.

Please let us know if you have any questions or would like to discuss any of these items. We would be very happy to organize a call with you to discuss our comments and to answer any questions you might have. We also look forward to continued engagement in this process and to providing further and more detailed comments on future drafts.

Finally, I'd like to refer you also to two of our 2019 papers on the subject of a US privacy law: (1) Ten Principles for a Revised US Privacy Framework[10] and (2) Learning from the GDPR: What Elements Should the US Adopt?[11]

Sincerely,

Matt Starr
Privacy & Public Policy Manager, CIPL

[10] Ten Principles for a Revised US Privacy Framework, March 21, 2019, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_principles_for_a_revised_us_privacy_framework__21_march_2019_.pdf.
[11] Learning from the GDPR: What Elements Should the US Adopt?, January 25, 2019, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_paper_-_learning_from_the_eu_gdpr_-_what_elements_should_the_us_ado....pdf.