Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

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

RE: The Uniform Law Commission's Collection and Use of Personally Identifiable Data Act

Dear Mr. McGeveran:

On behalf of Microsoft, I am writing to support the work of the Uniform Law Commission's (ULC) Collection and Use of Personally Identifiable Data Committee to develop model comprehensive privacy legislation. We find ourselves confronted with a conundrum. Technology has improved and transformed the way we live, work, and play. It has also left us awash in data. On the one hand, our ability to harness the power of data has brought progress and made innovation and the digital economy possible. It has empowered billions of people to improve their lives, learn new things, and feel more connected. On the other hand, it has overwhelmed our privacy laws, rendering them obsolete and posing profound threats to the privacy of people everywhere. In short, we face an urgent need to modernize privacy law.

At Microsoft, we have long supported calls for robust privacy laws because we believe they are essential for the long-term health and viability of our business and our industry. Many consumers have lost faith that the technology industry will protect their personal information or look out for their interests. They no longer trust that technology has, on balance, improved their lives and made the world a better place. Earning back that trust is essential. It is essential to restoring the public's confidence in technology. It is critical if companies wish to continue to demonstrate that they deserve the opportunity to place remarkable new products and services in the hands of people around the world.

While there are certainly things that individual companies and the industry writ large can and should do to earn back the public's trust, above all, it requires more. It requires laws.

For these reasons, Microsoft has long called for the adoption of strong privacy laws. We have been calling for federal privacy legislation since 2005. We are the only major technology company to apply the consumer rights at the heart of the European Union's General Data Protection Regulation (GDPR) to consumers worldwide. We were the first to announce that we would apply the California Consumer Privacy Act (CCPA) to all U.S. consumers. And we have supported efforts to pass state legislation,

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

including the Washington Privacy Act (WPA) in our home state of Washington, in states across the country.

The Committee's draft legislation, the Collection and Use of Personally Identifiable Data Act ("the Act") would, if enacted, provide consumers with some of the strongest consumer privacy protections in the world. It would require companies to responsibly steward the personal data they collect. And it would, in many ways, help make U.S. privacy law interoperable with the growing consensus of global privacy laws. These are goals that everyone—consumers, businesses, and policymakers alike—should share.

We are offering these comments to assist the Committee as it continues to refine and improve the Act. We are also submitting redlined suggestions to the Act as an Appendix included with this letter. We would be happy to meet and discuss any questions about our feedback that the Committee may have.

I. Consumer Rights

Any comprehensive privacy law must provide consumers with certain rights to control their personal data. These rights lie at the heart of a growing consensus of privacy laws around the world, many of which are based upon the European Union's General Data Protection Regulation (GDPR). They include the rights to access, correct, delete, port, and opt out of the processing of personal data. We applaud the Committee for including these rights in the draft Act. We have more specific comments to share regarding the opt out right, below.

A. The Right to Opt Out

We agree that consumers' right to opt out of data processing must include the ability to opt out of processing in furtherance of targeted advertising and profiling in furtherance of certain consequential decisions. Those activities continue to raise serious privacy concerns for consumers, and for that reason, we would encourage the Committee to continue to design the Act's opt out right to cover both targeted advertising and consequential profiling.

We also support requiring affirmative or opt-in consent to process sensitive data for targeted advertising or consequential profiling, and in fact, we would support opt-in consent for all processing of sensitive data.

B. Creating a Universal Opt Out Standard or Control

We would also encourage the Committee to include language that would enable the creation of a universal opt out control, so that consumers could exercise their right to opt out of the processing of their personal data for all controllers in one place and at one time. Even if consumers are granted the right to opt out, the sheer number of controllers who collect and use consumer data would make it

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

extremely onerous for consumers to exercise that right if forced to do so one controller at a time. A global mechanism, such as a browser control, an operating system setting, a universal Do-Not-Track registry, or some other means, would empower consumers and make the opt out right more effective. Moreover, if it is implemented through a rulemaking process to ensure that it is applied neutrally across platforms, businesses, and business models, and that it reflects an actual, affirmative choice made by a consumer, it would operate in a manner that is fair and evenhanded for all stakeholders in the ecosystem. We have included draft language to accomplish these things in the Appendix included with this letter.

II. Affirmative Duties

Providing consumers with rights to control their data is necessary, but by itself insufficient, to protect consumers' privacy today. Solely granting consumers rights would effectively place the burden of regulating privacy on the shoulders of each and every consumer, requiring them to make informed choices about which rights to exercise, with whom, and when. In view of the sheer volume of decisions that a consumer would face with respect to every company behind every app, every website, and every service that the consumer encounters across the Internet, that model of privacy governance (the "informed consent" model) is completely unrealistic. Companies must also shoulder responsibility for protecting the privacy of consumers' personal data, and for that reason, any comprehensive privacy law must also impose affirmative obligations on companies to steward the data they collect responsibly.

A. The Duties of Purpose Specification, Data Minimization, Secondary Use, Transparency, and Data Security

For these reasons, we support the Committee's efforts to include affirmative duties on controllers in the Act. Specifically, we support the duties of purpose specification, data minimization, transparency, and data security. We have some suggested language tweaks to these duties—please see the Appendix included with this letter.

B. The Duty of Loyalty

We also support the Committee's effort to include a duty of loyalty, and would suggest that the Committee articulate the duty as follows, which we view as being more robust and protective of consumers than the language in the draft Act:

> (7) *Duty of Loyalty*. A controller shall not process personal data in any way that:
>
> (a) will unfairly disadvantage consumers considering the benefits of such processing, the risk of harm to consumers, and the ability of the controller to mitigate any potential harm or detriment to consumers;
> (b) is reasonably likely to result in foreseeable harm to a consumer; or

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

(c) would be unexpected and highly offensive to a reasonable consumer.

For purposes of this section, "harm," includes, but is not limited to:
(i) physical harm;
(ii) identity theft and other direct or indirect financial loss or economic harms;
(iii) emotional or psychological harm, including anxiety, embarrassment, fear, unwelcome mental states, and other demonstrable mental trauma;
(iv) stigmatization or reputational harm; or
(v) other adverse consequences that would prove highly offensive to a reasonable person, such as an intrusion that would prove highly offensive to a reasonable person's privacy or seclusion, or the disclosure of private facts that would be offensive and objectionable to a reasonable person.

C. The Duty to Avoid Retaliation

We also support the inclusion of what the draft Act calls a duty not to "discriminate" against data subjects for exercising their rights. We would term this a duty to avoid "retaliation," and would encourage the Committee to articulate this right as the WPA did this past session. The WPA's language reflected substantial input from U.S. Retailers and certain consumer organizations to ensure that it would protect consumers' ability to exercise their rights while also permitting the continued operation of appropriate loyalty programs that are offered on fair and reasonable terms.

D. Additional Duties That We Would Recommend

Finally, we would recommend that the Committee strengthen the Act further by including the following affirmative duties:

- **A Duty of Non-Discrimination:** the Act should prohibit controllers from processing personal data on the basis of certain characteristics in a manner that unlawfully discriminates against consumers. A similar duty was included in a federal privacy bill recently introduced by Senator Maria Cantwell, the Consumer Online Privacy Rights Act.[1]

- **A Duty of Consent for Sensitive Data:** the Act should require controllers to obtain consent from consumers to process sensitive data. This would align the Act with the GDPR and other privacy laws around the world.

- **A Duty Regarding Secondary Use**: the Act should limit controllers' ability to process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which such personal data are processed, unless the controller obtains the consumer's consent.

[1] See section 108 of the Consumer Online Privacy Rights Act, available here: https://www.cantwell.senate.gov/download/copra-bill-text.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

- **A Duty of Confidentiality:** the Act should prohibit controllers from disclosing personal data except as consistent with the obligations under the Act.

- **A Duty to Avoid Abusive Trade Practices:** we would encourage the Committee to take a page from the Consumer Financial Protection Bureau and prohibit controllers from designing their products, services, or terms in a way that would materially interfere with or take advantage of consumers' ability to understand the risks, costs, or conditions of a product or service. See the Appendix included with this letter for our recommended language.

III. Definitions

A strong comprehensive privacy law must have strong definitions, and in general, the draft Act's definitions are comprehensive, clear, and robust. We would offer the following comments to refine and improve several of the definitions.

A. The Definition of "Deidentified"

Since deidentified data is outside the scope of the bill's rights and obligations, data must meet a very rigorous standard in order to qualify as "deidentified." We would encourage the Committee to consider making the definition more closely aligned with the longstanding approach to deidentification taken by the Federal Trade Commission, which is not only well known but also enjoys support from a broad range of stakeholders. See the Appendix included with this letter.

B. The Definition of "Personal Data"

Privacy legislation must define "personal data" broadly so that it covers the ways in which modern data sets are often stored (e.g., in association with cookie IDs or other hashed or online identifiers). To that end, "personal data" must be defined to include not only data that "identifies" a person or relates to an "identified" person, but also data that relates to an "identifiable person," meaning one who can be identified "directly or indirectly," including through the use of cookie identifiers or other online IDs.

Although it uses slightly different terminology, we read the draft Act's definition of "personal data" as being functionally equivalent to the definition included in the GDPR, which is a good thing. For the purpose of consistency, the Committee may consider adopting the GDPR's definitions of "personal data" and "identified or identifiable natural person," which would get the draft Act to essentially the same place substantively while using the same terminology as the GDPR and other global privacy laws.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

C. The Definition of "Profiling"

We applaud the Committee for drafting a definition of "profiling" that is balanced and robust. We also believe that consumers should have the ability to opt out of profiling in furtherance of consequential decisions about them, as the Act currently provides.

D. The Definition of "Public[ly] available data"

We would caution the Committee against expanding the Act's exemption to the definition of "personal data" for "public[ly] available data." This would include any efforts to expand the definition of publicly available data to include information that is made widely available online or via the media.

We raise this note of caution for several reasons.

First, inserting exemptions to the definition of "personal data" is strong medicine and should be carefully scrutinize because it renders such data completely unregulated. Accordingly, such an exemption should be applied only if the exempted information truly poses little to no privacy risk to consumers or is perhaps outweighed by other legitimate goals or interests. It has been argued that publicly available information must be exempted from privacy laws to avoid conflict with the First Amendment. But even if it is assumed that the First Amendment might preclude the application of some privacy rights to some information some of the time, exempting all publicly available information from all privacy rights and obligations all of the time is unwarranted. It would be overbroad and unnecessary to avoid any purported First Amendment conflicts. For example, would the First Amendment truly bar a consumer from asking a company to disclose whether it is holding personal information that it obtained about the consumer from government records? Would it really prohibit a consumer from asking the company for a copy of personal information about the consumer that it collected online, or from asking the company to correct such information if it is inaccurate or incorrect?

Second, it is not necessary to protect the First Amendment by expressly inserting exemptions into state statutes. Indeed, the First Amendment is in need of no defense. If a provision in a state law is found to conflict with the First Amendment, the First Amendment will obviously prevail by virtue of the U.S. Constitution's Supremacy Clause. That will remain true regardless of whether the law contains an express exemption for public information.

Third, completely exempting information that has been published on the Internet or otherwise made widely available in the media from the bill would create an enormous loophole in the bill's protections.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

E. The Definition of "Sensitive Data"

The definition of sensitive data should be expanded to include "specific geolocation information." Location information can reveal incredibly sensitive details about individuals' lives, and as such, the law should require affirmative consent before such data is processed.

IV. Data Protection Assessments

We support the imposition of a broad requirement on controllers to conduct a risk assessment of all of its data processing activities. In our view, conducting data protection assessments is a best practice and would help controllers improve their data hygiene, invest more in privacy compliance, and professionalize their approach to data protection. If the Committee is inclined to narrow the obligation, we would encourage it to require that assessments be done of all activities that pose a heightened risk of harm to consumers or have otherwise given rise to heightened privacy concerns. That would include, at minimum, the processing of personal data in furtherance of targeted advertising, profiling in furtherance of consequential decisions about consumers, the processing of sensitive data, and any processing activities that present a heightened risk of harm to consumers.

However, imposing a requirement to conduct data protection assessments on companies in their role as *processors*, as the Act currently does, reflects a fundamental misunderstanding of the role that processors play. Requiring processors to conduct data protection assessments seems to imply that processors are primarily responsible for, or have insight into, the decisions that are made regarding how and why data is processed. But by definition, processors may process personal data only on behalf of a controller and only pursuant to explicit instructions imposed by a binding contract. Processors do not retain the authority to make their own decisions regarding the purposes and means of processing personal data, and in fact, oftentimes do not even know what data controllers have asked them to process. For those reasons, controllers are the appropriate entities to conduct data protection assessments and evaluate the benefits and risks of what is being done with data.

We would recommend that the Committee require processors to provide documentation of its underlying processing activities, as necessary for the controller to conduct its data protection assessments. This would help ensure that controllers have all of the information they need to perform a proper assessment of their processing activities, including processing conducted on the controller's behalf by processors. The Committee could also consider imposing a requirement on processors to conduct assessments of their data security safeguards, as that is something that all companies, regardless of whether they are acting as a controller or a processor, could and should do.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

V. Obligations According to Role

We applaud the Committee for adopting the approach taken by the GDPR, the CCPA, and privacy laws around the world to define the obligations applicable to entities according to roles that they play in the online ecosystem—i.e., controllers and processors. We also applaud the Committee for attempting to spell out more expressly, and in a manner that is similar to the GDPR, the obligations that processors have viz a viz controllers. To that end, we would encourage the Committee to consider adopting the language from Section 5 of the WPA. That language was the product of substantial input from U.S. Retailers and, in our view, its inclusion could help garner additional support for the Act. See the Appendix included with this letter for suggested language.

VI. Data Privacy Officer

We support the Act's requirement that controllers designate a data privacy officer. Such a requirement is a best practice and will help controllers strengthen and professionalize their approach to data protection.

VII. Data Privacy Commitment

We understand that the Committee included the section on Data Privacy Commitments as a means of affording companies a safe harbor from enforcement. However, as drafted, the section would impose mandatory, bureaucratic, process-based obligations on companies that would appear to serve no meaningful function beyond what the Act's transparency and data privacy assessment obligations would already accomplish. We recommend that the Committee delete section 8.

Instead, we would recommend that the Act require controllers to maintain internal controls and reporting structures to ensure that senior management officials are actively involved in assessing the risks posed by the controller's processing activities and in making decisions that implicate compliance. This idea was included in the federal privacy bill released by Senator Roger Wicker, the United States Data Privacy Act of 2019.[2]

VIII. Exemptions for Data Regulated by Other Laws

The Committee has proposed exempting certain information that is regulated by existing federal statutes, and we understand that it may consider inserting additional exemptions. We would urge the Committee to proceed with caution and carefully scrutinize all proposed exemptions for information regulated by other laws. If done improperly, such exemptions could create loopholes in the bill's requirements and leave important categories of information subject to weak or minimal protections.

[2] See section 302 of the United States Data Privacy Act of 2019, available here: https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

Consequently, when considering proposed exemptions for information regulated by other laws, we would encourage the Committee to examine the protections afforded by such laws and incorporate the exemptions only if the Committee concludes that the other laws provide consumers with sufficient protections (or perhaps with protections that are comparable to those in the draft Act).

Furthermore, to the extent that the Committee incudes exemptions based upon other privacy laws, the exemptions should apply to the specific information and activities regulated by the other laws, and not to entities. Otherwise, if the exemptions applied to entities, they could effectively permit a large organization to evade the Act's requirements altogether (and immunize processing activities that are not regulated by other privacy laws) simply because a single division in the organization or a narrow category of the organization's processing activities is subject to another privacy law.

IX. Exceptions

As the Act acknowledges, there are certain limited situations where a controller may be required to maintain personal data, for example, to comply with other laws, protect against cybersecurity threats, prevent fraud, or otherwise ensure that its technology is working properly. We would recommend that the Committee include a few additional provisions in Section 3 to ensure that companies retain the ability to comply with law and perform internal operations to improve and provide its services. We would further recommend that the Committee restrict these exceptions by expressly clarifying that the duties of purpose specification, data minimization, and secondary use all apply to data processed under the exception, and that any data processed pursuant to the internal operations exception not be disclosed to third parties. We would also recommend that the Committee go even further by prohibiting the use of any data processed under the internal operations exception for profiling of any kind.

X. Enforcement

Enforcement, and specifically whether privacy legislation should provide for enforcement by Attorneys General or for private rights of action, continues to be a polarizing and controversial issue. More than anything else, this issue derailed efforts to pass the WPA in Washington State in 2019 and 2020. We appreciate the Committee's efforts to forge a path forward on this issue. We believe that a more nuanced, detailed discussion of the full panoply of enforcement options, which could include regulatory actions, administrative hearings, alternative dispute resolution, injunctive relief, rights to cure, actions under consumer protection or UDAP statutes, and other options, is needed. We would encourage the Committee to put a pin in enforcement and help facilitate a more robust and nuanced discussion on the issue with a broad range of interests and stakeholders at the table. We would be happy to participate and help the Committee in that effort.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

XI. Conclusion

We are committed to working with the Committee to develop legislation that would provide U.S. consumers with robust privacy protections and allow industry to innovate. Please consider us a resource if and when you think we can be of assistance.

We would be happy to discuss any questions that the Committee may have regarding our feedback. Thank you for your consideration.

Respectfully submitted,

Ryan P. Harkins
Senior Director, Public Policy
Microsoft Corporation