Computer & Communications Industry Association
Tech Advocacy Since 1972

October 1, 2020

Via Email: access.privacy@ontario.ca

Manager of Access and Privacy Strategy and Policy Unit
Ministry of Government and Consumer Services
Enterprise Recordkeeping, Access and Privacy Branch
134 Ian Macdonald Blvd.
Toronto, Ontario
M7A 2C5

Re: Reforming Privacy in Ontario's Private Sector (Tracking number 20-MGCS015)

Dear Privacy Consultation Manager:

Pursuant to the public consultation issued by the Ministry of Government and Consumer Services (the Ministry), the Computer & Communications Industry Association (CCIA) submits the following comments on protecting privacy and supporting Ontario's innovation economy.[1]

CCIA is an international, not-for-profit association representing a broad cross section of computer, communications and Internet industry firms. CCIA remains dedicated, as it has for over 45 years, to promoting innovation and preserving full, fair and open competition throughout our industry. Our members employ more than 1.6 million workers and generate annual revenues in excess of $870 billion.[2]

Given the scope and complexity of issues related to consumer data privacy, the enactment of any comprehensive privacy regulation will require sufficient input from all stakeholders and the development of clear definitions to ensure effective implementation. Therefore, CCIA applauds the Ministry for conducting this consultation and for seeking broad engagement from stakeholders and the public on ways to advance consumer privacy, avoid unnecessary burdens, and protect both prosperity and innovation. Balanced data privacy measures that align with individuals' expectations can protect people and communities and support the consumer trust that enables the digital economy. CCIA presents the following principles for protecting privacy

[1] Ontario Regulatory Registry, "Public Consultation - Reforming Privacy in Ontario's Private Sector" (Aug. 13, 2020), https://www.ontariocanada.com/registry/view.do?language=en&postingId=33967.
[2] A list of CCIA members is available at: https://www.ccianet.org/about/members/.

and promoting innovation in response to the Ministry's discussion paper to help guide consideration of private sector privacy reform in Ontario.[3]

I. *Transparency*

Consistent with requirements under the Personal Information Protection and Electronic Documents Act (PIPEDA), organizations should be transparent about the types of personal information that they are collecting, how it is processed, and under what circumstances they may share it.[4] As the Ministry notes, privacy statements written in dense legal jargon can deter engagement[5] and may fail to result in appropriate understanding on the part of consumers. Making relevant information about data processing practices readily available and accessible to users is crucial for enabling consumers to choose what services they wish to do business with and for promoting trust in the digital economy.

Organizations that process personal information are developing new mechanisms and procedures for actively informing individuals of data collection and use practices by making relevant information available in actionable ways. For example, emerging approaches to transparency include layered privacy notices, inline controls, and just-in-time notices.[6] The promulgation of prescriptive transparency and notice requirements could lead to longer and less intelligible notices, interrupt user experience, fail to account for different user interactions across technologies, and contribute to "click fatigue," reducing the overall effectiveness of transparency efforts.[7] Therefore, modern privacy regimes should support flexibility for organizations in providing accessible, relevant notices that are appropriate for the context of a particular product or service.[8]

---

[3] Ministry of Government and Consumer Services, "Ontario Private Sector Privacy Reform" (Aug. 13, 2020) *hereinafter* "Discussion Paper"
https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45716.

[4] Personal Information Protection and Electronic Documents Act (PIDEDA), S.C. 2000, c. 5 at 4.2; 4.8.

[5] Discussion Paper at 4.

[6] *See*, Florian Schaub, Rebecca Balebako, Adam L. Durity & Lorrie Faith Cranor, "A Design Space for Effective Privacy Notices," Symposium on Usable Privacy and Security (2015),
https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf.

[7] *See e.g.*, Government of Canada, "Strengthening Privacy for the Digital Age" (May 21, 2019) ("Requiring too much detailed information in the consent process can overwhelm individuals or become yet another screen on a device to click-through in the rush to get to the product or service.")
https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

[8] CCIA appreciates that the Ministry is considering alternative models to transparency and consent. To promote effective transparency, regulators should consider collaborative approaches such as regulatory "sandboxes" for supporting the development of modern transparency mechanisms focused on individuals' needs and experiences across different technologies. *See e.g.*, Erin Egan, "Communicating About Privacy: Towards People-Centered and Accountable Design," Facebook (July 2020),
https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf.

II. *Consent*

CCIA supports the Ministry's goal of enabling greater user control over their personal information and agrees that in the modern digital economy, "customers cannot be expected to consent each time their information is collected."[9] Requiring specific consent for every aspect of data processing would create an overly complex and confusing experience for users and divert from the overall goals that privacy frameworks aim to achieve. Furthermore, as potential beneficial uses or insights drawn from data may not always be known at the point of collection, obtaining specific, affirmative consent for each secondary use of data could severely curtail innovative reuse of data, socially beneficial research, and the development of emerging technologies such as machine learning and artificial intelligence. Therefore, in order to effectively empower consumers and support data-driven innovation, CCIA recommends that any requirements for receiving "opt-in" consent be employed where a use of data is unexpected in the context of a service or presents a significant impact to individual privacy.

CCIA appreciates the recognition of the need to clarify exceptions to consent requirements for secondary uses of data, such as using de-identified or derived information or data processing in the public good.[10] In order to ensure that consent requirements are tailored to support informed choices and greater control over data, the Ministry should consider additional exceptions, such as uses that are consistent with the original purpose of collection, internal research and analytics, and "common uses of personal information for standard business activities."[11] Finally, consistent with emerging private sector privacy regimes, CCIA recommends delineating alternative valid bases for processing data in addition to consent, such as for the performance of a contract, compliance with a legal obligation, in cases where the vital interests of an individual are at stake, and for the purposes of a legitimate interest.[12]

III. *Deletion*

The creation of a right to request the deletion (and, where practical, correction) of personal data held by a covered organization would support the Ministry's goal of promoting individuals' control over their personal information. Any right to deletion should also account for implementation challenges, afford organizations appropriate time to verify and process requests, and not override other legal obligations such as record-keeping obligations for fraud detection. It is also appropriate to include exceptions for de-identified and unstructured data as well as data that implicates the personal information of third-party users.

---

[9] Discussion Paper at 4.
[10] Discussion Paper at 4.
[11] *See e.g.*, Government of Canada *supra* note 7.
[12] *See e.g.*, General Data Protection Regulation (GDPR) Art. 6.

CCIA cautions against conflating a right to deletion (discussed above) with a so-called "right to be forgotten" (RTBF) or de-indexing from online search results or references. Any formulation of a RTBF would be tension with fundamental rights including freedom of expression and freedom of press.[13] Further, the establishment of a RTBF would open the door to widespread private-censorship and suppression of lawful content within and potentially beyond Ontario. Even with exceptions contemplated by the Ministry, companies facing liability for failing to respond to RTBF requests may default to removing information, reducing Ontarians' access to information relative to other Canadians and their peers in countries that value free expression.[14]

IV. *Portability*

Data portability refers to the right of individuals to access and receive the personal information that they have provided to an organization for export in a machine-readable format. Balanced and reciprocal data portability mechanisms benefit competition and innovation by reducing the transactions costs of users to move between data-enabled products and services. However, enactment of prescriptive data portability requirements could create compliance costs that advantage incumbents over smaller competitors and establish new barriers to market entry.[15] Furthermore, if data transfer mandates extend to analytic information and insights generated by an organization, portability could allow some companies to free ride on the efforts of others, thereby chilling the incentive to develop new innovative services.

The Ministry should ensure that the development of data portability standards across different sectors promotes user autonomy without negative impacts to privacy. Extending portability to data categories that pertain to multiple individuals such as contact lists, photos, and social information would put individuals at risk of having personal information transferred to an unknown third party without knowledge or consent.[16] Therefore, portability mechanisms should recognize that consumer expectations of the availability of their information for third-party transfers may vary across services and types of information. Furthermore, as any transfer of personal information presents inherent privacy and security risks, organizations require clear guidance on procedures for authenticating and securely fulfilling portability requests.

---

[13] Candian Charter of Rights and Freedoms, 1982, s 2(b).
[14] *See* Eloïse Gratton & Jules Polonetsky, "Privacy above all other Fundamental Rights? Challenges with the Implementation of a Right to be Forgotten in Canada" (Apr. 28, 2016), https://fpf.org/wp-content/uploads/2016/04/PolonetskyGratton_RTBFpaper_FINAL.pdf.
[15] Peter Swire & Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," 72 Md. L. Rev. 335, 356 (2013).
[16] *See* Kevin Bankston, "How We Can 'Free' Our Facebook Friends," Techdirt (July 11, 2018), https://www.techdirt.com/articles/20180706/13460040185/how-we-can-free-our-facebook-friends.shtml.

Given these considerations, data portability tools are best developed through open, consensus-based standards in response to consumer interests and needs. Data portability mechanisms should (1) allow users to download and move data they have provided to the service, (2) afford users control over how and when the tools are used; and (3) be tailored to the privacy and security expectations of individuals and practical and technical considerations of a particular industry.

V. *Oversight, Enforcement, and Fines*

Data protection regimes that effectively promote consumer privacy interests and control of personal information require risk-based enforcement mechanisms to stop violations and remediate unlawful behavior. While organizations should be expected to meet certain baseline requirements for protecting privacy, reasonable data protection practices may differ across covered organizations. Context, including an organization's scale and resources, the sensitivity of the data it holds, and its uses for that data, should inform the measures that it puts in place to protect data. Therefore, CCIA supports the Ministry's recognition that different compliance strategies are appropriate for small, medium, and large organizations and that a broad toolkit exists for promoting compliance including "education, research, guidance, and advisory services, to regulatory sandboxes."[17]

CCIA recommends that the Ministry consider additional proactive and collaborative privacy compliance measures such as safe harbors and certifying codes of conduct. These accountability mechanisms support industry-specific application of privacy rules, promote the development of best practices beyond minimum statutory requirements, and assist organizations' predictability in meeting their compliance obligations. Finally, in order to avoid chilling innovative data practices (especially by small and medium-sized entities), any fining authority should be proportionate to the risk of harm caused by the unlawful conduct and applied to willful or repeated violations.

VI. *Application to Non-Commercial Entities*

Privacy risks to individuals resulting from the processing of personal data are based on the sensitivity and use of the information at issue and are not limited to processing by commercial organizations. Therefore, modern privacy frameworks should apply to all organizations or entities that process personal information, including non-profits, regardless of whether they have a direct or commercial relationship with an individual whose information they hold.

[17] Discussion Paper at 6.

VII. *Deidentified Personal Information*

Enabling effective compliance with a data protection regime requires that organizations have a clear understanding of what data holdings are subject to privacy requirements. Therefore, it is important to carefully define "covered information," which should extend to personal data under the control of a covered organization, that is not generally available to the public through lawful means, and is linked or practically linkable to a specific individual, or linked to a specific device or account that is associated with or routinely used by an individual.

The use of de-identification, anonymization, and data aggregation techniques can effectively eliminate the risk of harm from data processing, while still permitting beneficial use and analysis. Therefore, it is appropriate to carve out de-identified data from data protection requirements, which has the added benefit of incentivizing organizations to handle data more in privacy protective ways. The Ministry should consider engaging with experts and stakeholders to develop guidance on effective technical standards and procedures for de-identifying datasets.

VIII. *Additional Considerations for Privacy Governance*

CCIA offers the following additional considerations for developing effective consumer privacy governance regimes to support practical implementation of data protection principles and the preservation of data-driven innovation.

A. Promote Interoperability Between Privacy Frameworks

In the modern digital economy, the transfer of data across jurisdictional borders connects businesses to the global marketplace and supports secure and effective data processing. The emergence of a patchwork of divergent privacy frameworks across Canada would raise compliance burdens for organizations and present challenges for consumers seeking to understand and exercise their privacy rights. Therefore, both organizations and individuals benefit from the ability for data controllers to maintain consistent compliance programs based on widely shared principles of data protection. Any new privacy protection regime should account for and promote harmonization with emerging national and international concepts and practices in data protection and take steps to avoid unnecessarily encumbering organizations' ability to engage in interprovincial trade and process data within and beyond Canada.

B. Recognize the Role of Service Providers

Privacy frameworks should recognize the distinction between "data controllers" that direct the collection and processing of personal information and "data processors" such as

service providers who may process information on behalf of another organization.[18] These organizations are differently situated with respect to their relationship with data subjects and have distinct roles for effectively protecting privacy and implementing consumer rights. Therefore, privacy law should set clear expectations and responsibilities regarding the onward transfer of data to third-party processors.

C. Forward looking

As the Ministry's announcement notes, privacy frameworks should retain necessary flexibility so as to remain relevant and effective with the development of new technologies and business practices. Therefore, a comprehensive consumer privacy regime should be: (1) technology-neutral, avoiding narrow mandates regulating specific technologies and (2) outcome oriented, enabling organizations to make adjustments according to the needs of individuals and evolving technology.

Conclusion

CCIA appreciates the opportunity to submit these comments in response to the Ministry's consultation on reforming privacy in Ontario's private sector. CCIA hopes that through this comment process, policymakers will gain more information from stakeholders and the public, and that policy outcomes will: (1) aim to protect data through a robust, technology-neutral framework for assessing and managing privacy risks to individuals and organizations; and (2) seek to promote innovation in both digital services and privacy protection.

Respectfully submitted,

Keir Lamont
Policy Counsel
Computer & Communications Industry Association

[18] *See e.g.*, GDPR Chapter 4 "Controller and processor."