1 October 2020

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

Vía email: access.privacy@ontario.ca

The Information Accountability Foundation (IAF) appreciates the opportunity to comment on the Ontario government's consultation to improve the province's privacy protection laws. The IAF is a global non-profit organization that conducts research and education on data protection and privacy from an accountability perspective. It is the incorporation of the Global Accountability Dialog that operationalized the accountability principle in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data for application in a digital economy and society.[1] The IAF has conducted research in Europe, Asia and the Americas, including three projects in Canada.[2] Next generation privacy legislation is an IAF focus area[3], and it is from that perspective that the IAF is providing comments.

Ontario currently does not have regulations for privacy in the private sector and neither the Canadian Charter of Rights and Freedoms (Charter)[4] nor the Ontario Rights Code (Code)[5] specifically mention privacy or the protection of personal information, although the Charter does afford protection under Section 7 of the Charter (the right to life, liberty and the security of the person).[6] Moreover, the Charter only applies to governments and not to private individuals, businesses or other organizations.[7] As a result, Ontario relies on the federal Personal Information Protection and Electronic Documents Act (PIPEDA) which in its Purpose section "recognizes the right of privacy of **individuals** with respect to their personal information" but does not define the right of privacy.[8] PIPEDA's reference to "individuals"

[1] https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm
[2] Report for the Big Data Assessment for Canadian Private Sector Organizations Project; Report for the Comprehensive Assessment Oversight Dialog Canadian Ethical Data Review Boards Project; A Path to Trustworthy People Beneficial Data Activities
[3] IAF has drafted model privacy legislation with 2030 in mind. A summary of this model legislation can be found here.
[4] https://laws-lois.justice.gc.ca/eng/const/page-15.html.
[5] R.S.O. 1990, c. H. 19
[6] A Guide for Individuals Protecting Your Privacy, An Overview of the Privacy Commissioner of Canada and Federal Privacy Legislation, https://www.priv.gc.ca/en/about-the-opc/publications/guide_ind/
[7] Human Rights in Canada, Canadian Human Rights Commission, https://www.chrc-ccdp.gc.ca/eng/content/human-rights-in-canada
[8] PIPEDA S.C. 2000, c. 5.

points out that it is not only the right of single individuals, but also the privacy right of groups of individuals and society in general, that is protected.

Most rights and freedoms are fairly straight forward, but scholars have had a hard time defining the right of privacy. So, rather than define the right, it is simpler to define the interests that the right encompasses. There are three interests:

- The first is the interest in seclusion. All of us need a space where we are free of observation or intrusion into our private lives. This interest in seclusion rests on privacy within a household and the papers and the records associated with that household. In many ways our interest in seclusion has been eroded by the observational nature of modern society, where a record of behavior can be created without a legacy paper record.
- The second is the interest in an individual defining his- or herself and in not being defined by the digital tracks he or she leaves behind. This interest is reflected in actions related to the individual's autonomy or ability to control the data that pertains to the reputation of the individual.
- The third is the interest in fair processing. This interest relates to the individual's interest in fair treatment, absent inappropriate discrimination, with decisions based on accurate data. As data have become fundamental to the way processes and machines work (e.g. internet-of-things), more of the work of privacy agencies and privacy professionals has been dedicated to fair processing.

How technology interfaces with those three interests is very different today than it was 20 years ago when PIPEDA was enacted. Privacy is not a singular right. PIPEDA's purpose makes clear it is not only the "right of privacy of individuals with respect to their personal information" but it is also "the need of organizations to collect, use or disclose [process] personal information for purposes that a reasonable person would consider appropriate in the circumstances" that is being recognized.[9]

There are risks and benefits to people that have come with the Internet, smart phones, connected cars, advanced analytics and an internet of everything. When the enactment of privacy legislation is considered, how privacy intersects with other rights and freedoms needs to be considered. The rights and freedoms set forth in the Charter and the Code are not absolute,[10] and as PIPEDA articulates, neither is privacy.

Moreover, individuals have other interests that are just as important as the privacy interests. Those interests include better health and education and better employment and business opportunities. They also include the interest in accurate information and in making decisions based on data validated facts. Sometimes those interests are best served when aggregated with the interests of other individuals into societal interests. For example, while an individual has an interest in how health records might impact reputation and standing, the individual also has an interest in that data being used in a protected manner for healthcare research. That interest in better healthcare through research is shared with all Ontarians.

Quality privacy law links one or more of these interests with privacy interests. To be successful, privacy law must include processes that facilitate analysis of the full range of interests and the full range of

[9] PIPEDA, Section 3
[10] Charter, Part 1

stakeholders. This makes writing and implementing privacy law hard, but it also protects Ontarians while they receive the benefits of an information-based economy. That is why the OECD Accountability Principle, that is the foundation for PIPEDA, has been updated to recognize ever more complex assessment processes that must be demonstrable. While the IAF shares the view that the time is now for private sector privacy legislation for Ontario, it believes the legislation should include topics that are not included in the topics in the Discussion Paper.[11] The IAF's comments are all at a high level and suggest the legislation should be structured with provisions that facilitate a vibrant society.

Next generation privacy law also should proportionately balance the multiple interests and numerous rights and freedoms. In particular, the legislation should be structured in a manner where the full range of rights and freedoms are addressed in a manner that matches remedies so that they tie proportionally with the privacy interests of seclusion, autonomy, and fair processing, with other individual interests and with the rights and freedoms in the Charter and Code. Proportionality is typically framed as an administrative requirement for government, where the fundamental rights and freedoms of individuals are compromised by the power of the state as a user of data pertaining to people. Proportionality is different when framed as a private sector requirement. It links to advanced data processors balancing the full range of interests of all stakeholders - individuals, groups of individuals, society and organizations. Responsible processing of data requires balancing of the multiple rights and freedoms and the numerous interests of all the stakeholders that may be impacted by processing or failing to process data.

The Legislation Should Include a Forward-Thinking Articulation of Accountability

The topics in the Discussion Paper do not include the concept of accountability. Perhaps this omission is because PIPEDA contains an accountability principle. However, as mentioned above, PIPEDA is 20 years old. The guidance on what it means to be an accountable organization[12] is eight years old. The Essential Elements of Accountability were adopted by a global dialog in 2009[13] and are the basis for how accountability through a comprehensive privacy management program has been described in Canada.[14] Accountability begins with the overarching principle that data should be processed by organizations in a responsible manner and that organizations should be answerable for that responsible processing. However, in the years that have passed since PIPEDA was enacted and the Accountability Guidance was issued, the complexity of data processing has increased. As that complexity increases, the accountability of organizations for that data processing must increase as well.

Furthermore, as the digital strategy of Canada reveals, data drive national economies. The goal of Canada's digital strategy is for Canadians to benefit from the opportunities that the digital economy offers while at the same time protecting them from the threats posed by the embrace of digital

---

[11] Ontario Private Sector Privacy Reform Discussion Paper (Discussion Paper), https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45105

[12] Getting Accountability Right with a Privacy Management Program (2012), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/

[13] A representative of The Office of the Privacy Commissioner, Canada, participated in defining the essential elements of accountability.

[14] Getting Accountability Right with a Privacy Management Program [hereinafter Accountability Guidance], https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/

technologies, including threats to the safety of personal data and to individual privacy.[15] Digital technologies are electronic tools, systems, devices and resources that generate, store or process data.[16] In order for Ontarians to benefit from this data driven age, Ontario needs an accountability framework that addresses and anticipates the benefits and detriments of digital technologies, especially those that operate without human involvement.

The IAF's work in Canada and other jurisdictions considers how the Essential Elements of Accountability might be updated for today's more complex and highly connected world. The Fair Processing Demonstrable Accountability Framework includes, among its requirements, an assessment process that balances the risk of harm and benefits to people of digital technologies. This Framework is based on Data Stewardship Accountability Framework which was featured in the Enhanced Data Stewardship Accountability Project that was conducted in partnership with the Privacy Commissioner of Hong Kong.[17] The IAF will be publishing further updates to address the elements of Fair Processing Demonstrable Accountability later in 2020. However, a summary version of these elements follows.

For example, demonstrable accountability elements, where the organization's responsibilities increase as the complexity of the digital age increases, should require:

- Organizational commitment to fair processing demonstrable accountability and the adoption of internal policies consistent with external criteria and established fair processing principles. As a matter of commitment, organizations should define fair processing values and/or principles which then are translated into organizational policies and processes. These principles should be organizationally derived and should be in addition to laws or regulations. They may go beyond what the law requires but should be aligned and not inconsistent with existing laws, regulations, or formal codes of conduct.
- Mechanisms to put fair processing policies into effect, including risk based adverse impact assessments, tools, training and education. Fair Processing Impact Assessments (FPIAs) should be required when advanced data analytics may impact people in a significant manner and/or when data enabled decisions are being made without the intervention of individuals. Where an analytical data driven use has potential impact at the individual level or at a higher level (e.g. groups of individuals and society), the benefits and adverse impacts should be explicitly defined and should be mitigated to the extent possible. Organizations should use a "fair processing by design" process to translate their fair processing principles and other policy requirements into their digital technology system design processes so that society, groups of individuals, or individuals themselves, and not just the organizations, gain value from data processing activities.
- Internal review processes that assess higher risk FPIAs and the overall fair processing program. Higher risk or higher impacting data initiatives, or where adverse impacts have not been sufficiently addressed, should be referred to more senior organizational decision-making group(s) for their review and approval. The escalation process should be based on and be part of the programmatic risk management approach and should address that issues raised as part of the FPIA have been resolved and that advanced data processing activities have been conducted as planned.

---

[15] Canada's Digital Charter in Action: A Plan by Canadians, for Canadians, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

[16] Education & Training, State Government of Victoria, Australia 2019

[17] https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Hong-Kong-Report-FINAL-for-electronic-distribution-10.22.18.pdf; https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Enhanced-Data-Stewardship-EDIA-FINAL-10.22.18.pdf

- Individual and organizational transparency and mechanisms for individual participation. The fair processing principles that govern the advanced data processing activities and that underpin decisions should be communicated widely, and processes should be proactively transparent wherever possible. Furthermore, all societal and individual concerns should be addressed and documented as part of the FPIA process, and accountability feedback mechanisms should be established.
- Means for remediation and external enforcement. Organizations should stand ready to demonstrate to the regulatory agencies with authority, including certifying bodies to which the organizations are subject, the soundness of internal processes, the propriety of advanced data processing activities, and when data processing may or does impact people in a significant manner.

New privacy legislation should address these elements of demonstrable accountability so that processes are established that place more responsibility on organizations as digital challenges of today and the future increase.

The Lawful Processing of Personal Information Should Not be Limited to Consent

In Canada, as a whole, consent has been a gating requirement, but the heavy lifting for protecting people while processing data has been by privacy management programs required by the accountability principle. When attempting to enhance privacy outcomes, it has often been attractive to fall back on consent by a person about data that pertains to that person as an attractive bright-line policy. In actuality, that approach transfers the risk associated with decision making from the organization processing data to the individual. Risk assessments should stay with the organizations processing the data and not passed on to the individual. That does not mean consent is not important. Consent is important, but it should not be the means for governing complex data processing.

In the 2016-2017 Report on Consent of the Office of the Privacy Commissioner, it was recognized that consent may be a poor fit in certain circumstances, e.g., where consumers do not have a relationship with the organization using their data and where uses of personal data are not known at the time of collection, or too complex to explain to individuals. Consent is a foundational element of PIPEDA. Legally, organizations must obtain meaningful consent to process an individual's personal information, subject to certain exceptions. When PIPEDA was adopted, interactions with businesses were generally predictable, transparent and bi-directional. Individuals understood why the company they were dealing with needed certain personal information. There were clearly defined moments when information collection took place and consent was obtained. But obtaining consent has become increasingly challenging and ineffective in protecting individuals in the digital environment. While there remains an important role for consent in protecting the right to privacy where it can be meaningfully given, complex information flows and business processes involving a multitude of third-party intermediaries, such as search engines, platforms, and advertising companies, have put a strain on the consent model; in the age of big data, the Internet of Things, artificial intelligence and robotics, it is no longer entirely clear to consumers who is processing their data and for what purposes; for individuals, the cost of engaging with modern digital services means accepting, at some level, that their personal information will inevitably be required to be collected and used by companies in exchange for a product or service.[18] Given the recognition that business relationships are no longer just bi-directional and that consent may no longer

[18] 2016-2917 Report on Consent. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1

always be practicable, it is outdated to draft legislation that is supposed to be modernizing to require consent as a condition to process personal information from the individual.

According to the Discussion Paper, Ontario is considering clarifying consent requirements that would include clarifying exceptions to consent. These may be instances where individual consent is not necessary, practicable or appropriate, such as when the collected data is used to benefit the individual or the overall public good (e.g. for purposes of research or innovation.) For all other processing of personal information, the organization would need to obtain affirmative, demonstrable, informed, and unambiguous consent.

Given that an expressed purpose of the Ontario legislation is to adopt a modern privacy law in order to be in alignment with the EU General Data Protection Regulation (GDPR), it would be prudent also to incorporate the lawfulness of processing set forth in Article 6 of the GDPR. Article 6 contains six legal means to process data, one of which is legitimate interests. Legitimate interest in the GDPR is more well defined than the reference to "data used to benefit the individual" in the Discussion Paper. Legitimate interest concerns processing "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[19] The recitals to the GDPR make clear that the processing of personal data strictly for the purposes of preventing fraud constitutes a legitimate interest of the data controller concerned, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest, where controllers are part of a group of undertakings or institutions affiliated to a central body, they may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data.[20] The recitals make it clear that the processing described in them are examples and that other circumstances that meet the requirements of the GDPR are permitted, i.e., those necessary for the purposes of the legitimate interests pursued by the controller or by the third party AND those not overridden by the interests or fundamental rights and freedoms of the data subject.[21] How Article 6 of the GDPR is drafted and specifically how legitimate interests is approached in the GDPR demonstrates how Ontario should approach expanding beyond consent as a basis for the processing of personal information.

Deidentified Personal Information and Data Derived From Personal Information Need a More Nuanced Approach

The IAF's Martin Abrams wrote a paper for an OECD workshop in 2014 that created a taxonomy of data based on origin.[22] The paper has been used to define data types in international discussions. The Discussion Paper combines data coming from third parties, data derived by arithmetic processes, and data that are algorithmic insights into the term derived data. The IAF paper places an emphasis on inferred data because of the predictive values that come from algorithms.

The Discussion Paper proposes that deidentified data should be personal data without any rationale. Every mechanism that obscures the link between a piece of data and the link to the person to whom the

[19] GDPR Article 6(e)
[20] GDPR Recitals 47 and 48
[21] GDPR Recital 47
[22] "The Origins of Personal Data and its Implications for Governance"

data pertains should be done so for a purpose. That purpose should not be to isolate the data from governance, but rather so it is part of the governance process. Obscuring linkages can protect individuals from being impacted when data is lost or stolen. It also can provide an extra governance step before the learnings from a processing are applied to an individual. The IAF suggests that the purposes for obscuring data be considered before enacting rules that define data governance.

Privacy Legislation Should Be Proportionate

In *R. v. Oakes,*[23] the Supreme Court of Canada set forth the proportionality test. This test should be considered when drafting privacy legislation. Thus, the following factors should be considered:

> First, the objective to be served by the measures limiting a Charter right must be sufficiently important to warrant overriding a constitutionally protected right or freedom.
>
> Second, the party invoking the first section must show the means to be reasonable and demonstrably justified. This involves a form of proportionality test involving three important components.
>
> - To begin, the measures must be fair and not arbitrary, carefully designed to achieve the objective in question and rationally connected to that objective.
> - In addition, the means should impair the right in question as little as possible.
> - Lastly, there must be a proportionality between the effects of the limiting measure and the objective – the more severe the deleterious effects of a measure, the more important the objective must be.

First, for reasons discussed in more detail above, the Discussion Paper's emphasis on increased consent is not carefully designed to achieve the objective in question and is not rationally connected to that objective - a privacy law suitable for the complexities of the digital age. Requiring consent for the processing of personal information in the complicated digital age, an information-based economy using computer or other technology devices as medium of communication,[24] is often impossible. Therefore, this type of privacy law is unlikely to be effective in meeting that need.

In addition, the legislation as envisioned in the Discussion Paper does not impair the right to privacy as little as possible. As also discussed above, the right to privacy consists of many interests. Over reliance on one of those interests, autonomy or consent, and no recognition of the other interests, seclusion and fair processing, impedes the ability to achieve a privacy law suitable for a challenging digital age.

Lastly, there is no proportionality between the effects and the objective. As further discussed above, privacy is not an absolute right. There must be consideration of how privacy interacts with other rights and freedoms of the individual, other individuals impacted by the processing and society as a whole. The IAF project paper "A Path to Trustworthy People Beneficial Processing" discusses looking at the interest of all stakeholders. In particular, there must be a consideration of the need of organizations to

[23] [1986] 1 SCR 103. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/117/index.do

[24] Adnan Rizal Harris, Issues in Digital Era, Research Gate, December 2016 https://www.researchgate.net/publication/328528038_Issues_In_Digital_Era/link/5bd275eba6fdcc3a8da64dd4/download

process personal information. The Purpose provision of Part I of PIPEDA[25] sets forth how to balance the right of privacy and the need of organizations to process personal information:

> "The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

The proposed legislation overemphasizes the need for individual consent to the processing of personal information and underemphasizes the organization's need to process personal information in the demanding digital age in an accountable fashion.

As discussed above, there is a less privacy invasive way of achieving the same end. There should be a modern articulation of accountability; legitimate interest should not be limited to an exception to consent and should be a well-articulated standalone basis for processing personal information; both de-identified and derived information should be considered in a more nuanced fashion; and there should be a proportionate balancing of rights and freedoms.

A recent articulation of proportionality is found in the Canadian guidance on COVID-19. In the Public health ethics framework: A guide for use in response to the COVID-19 pandemic in Canada,[26] it is stated under Minimising Harm:

> "**Proportionality**: potential benefits should be balanced against the risks of harm. Measures should be proportionate to the relevant threat and risks, and the benefits that can be gained. If a limitation of rights, liberties or freedoms is deemed essential to achieve an intended goal, the least restrictive measures possible should be selected, and imposed only to the extent necessary to prevent foreseeable harm."

Given the benefits of the digital economy that the Ontario Government wants to take advantage of, it is imperative that proportionality among rights, interests and freedoms and not proportionality within a right, interest or freedom, is balanced. When balancing the right of privacy and the need of organizations to process personal information, it is clear that the legislation contemplated in the Discussion Paper is not proportionate.

Concluding Remarks

Writing privacy legislation for the next generation is difficult. It must protect the full range of interests, rights and freedoms but still facilitate a digital economy. The IAF is confident that with an inclusive consultation process, quality legislation will be the outcome. The IAF team would be pleased to respond to questions. Please reach out to Martin Abrams at mabrams@informationaccountability.org.

[25] https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html#h-416888

[26] https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection/canadas-reponse/ethics-framework-guide-use-response-covid-19-pandemic.html