10 September 2020

The Information Accountability Foundation ("IAF") appreciates the opportunity to comment on the proposed privacy legislation introduced by the Quebec government for passage in the Quebec National Assembly. 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. The IAF conducted a dialog In Montreal on government use of data in 2014 with former Quebec privacy commissioner Jennifer Stoddart.[2] Next generation privacy legislation is an IAF focus area, and it is from that perspective that the IAF is providing these comments.

The IAF agrees with the Quebec government's assessment that now is the right time to update legislation enacted nearly thirty years ago. Quebec was an early Canadian adopter of private sector privacy law, enacting legislation in 1993. Quebec was a pathfinder because privacy is a fundamental right under the Quebec Charter of Human Rights and Freedoms and remains a fundamental right. Most fundamental rights are fairly straight forward. Not so privacy. In fact, scholars have a hard time capturing the essence of privacy in definitions. So, rather than define the right, it is often simpler to define the interests that the right encompasses. There are three interests:

- The first is the individual's 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 one may create a record of behavior without a legacy paper record.[3]
- The second is the individual's interest in defining his- or herself and not be defined by the digital tracks left behind. This is reflected in actions related to the individual's autonomy or ability to control the data that pertains to the reputation of the individual.[4]
- The third is the individual's 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 has become fundamental to the way processes and machines work (e.g.

[1] https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

[2] "Organizational Accountability, Government use of Private Sector Data, National Security, and Individual Privacy."

[3] Section 5 of Chapter I of Part I of the Quebec Charter of Human Rights and Freedoms provides: "Every person has a right to respect for his private life."

[4] Section 4 of Chapter I of Part I of the Quebec Charter of Human Rights and Freedoms provides: "Every person has a right to the safeguard of his dignity, honour and reputation."

internet-of-things), more of the work of privacy agencies and privacy professionals has been dedicated to fair processing.[5]

How technology interfaces with those three interests is very different today than it was 30 years ago. The law predates the 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 fundamental rights and interests needs to be considered. Privacy, while fundamental, is not an absolute right. Every individual has other rights and interests that are just as important. Those interests include better health and education, the right to be employed and create a business. They also include the right to information and to make 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 Quebeckers. Quality privacy law links one or more of those privacy interests and allows for proportionate balancing among all rights and freedoms.

While the IAF shares the view that the time is now for legislation, it believes the legislation could better balance the interests of all Quebeckers. The IAF's comments are all at a high level and suggest the proposed legislation should be structured with provisions that facilitate a vibrant society. In particular, the proposed legislation should be structured in a manner where the full range of rights and interests are addressed in a manner that matches remedies so that they tie proportionally with seclusion, autonomy, fair processing and other rights and interests. Proportionality is typically framed as an administrative requirement for government, where the fundamental rights 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 users balancing the full range of interests of all stakeholders. While the emphasis is on the many interests of the individuals to whom the data pertains, the responsible data user also considers the interests of other stakeholders that may be impacted by the processing or failure to process data.

The Articulation of Accountability Should be Forward Thinking

The proposed legislation introduces the concept of accountability and very specifically sets forth how accountability should be achieved through specific and specified obligations. However, the legislation does not define purpose and true function for accountability. Accountability begins with the overarching principle that data should be processed by organizations in a responsible manner and should be answerable for that responsible processing.

The proposed legislation does not describe the overarching objective for accountability, and its provisions are both incomplete and too specific for a bill that is supposed to modernize the framework applicable to the protection of personal information. The Essential Elements of Accountability were

[5] Section 10 of Chapter I of Part I of the Quebec Charter of Human Rights and Freedoms provides: "Every person has a right to full and equal recognition and exercise of his human rights and freedoms, without distinction, exclusion or preference based on race, colour, sex, gender identity or expression, pregnancy, sexual orientation, civil status, age except as provided by law, religion, political convictions, language, ethnic or national origin, social condition, a handicap or the use of any means to palliate a handicap."

adopted by a global dialog in 2009[6] and are the basis for how accountability through a comprehensive privacy management program has been described in Canada.[7] This proposed legislation falls short when matched with the essential elements, as one can see in the chart below, much less modernize them for the decades ahead.

2009 Essential Elements of Accountability	Quebec Proposed Legislation
Organisation commitment to accountability and adoption of internal policies consistent with external criteria	The highest-ranking officer of the company is responsible for the protection of personal information, and the title and contact information of the person in charge ("PIC") must be published. Governance policies and practices that ensure the protection of personal information (i.e. retention and destruction of information, roles and responsibilities, complaints processes), proportionate to the nature and scope of activities, must be established, implemented, approved by the PIC and published on the enterprise's website.
Mechanisms to put privacy policies into effect, including tools, training and education	An assessment of the privacy-related factors of any information system or electronic service delivery project must be conducted. From the outset of the project, the PIC must be consulted. The project must allow computerized personal information to be communicated in a structured, commonly used technological format. The PIC may suggest personal information protection measures applicable to the project, such as: - Appointment of a person responsible for the implementing of personal information protection measures, - Measures to protect personal information in any document regarding the project, - Description of the project participants' responsibilities regarding the protection of personal information; - Training activities for project participants on the protection of personal information

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

[7] Getting Accountability Right with a Privacy Management Program, 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/

Systems for internal, ongoing oversight and assurance reviews and external verification	
Transparency and mechanisms for individual participation	Governance policies and practices that ensure the protection of personal information (i.e. retention and destruction of information, roles and responsibilities, complaints processes), proportionate to the nature and scope of activities, must be established, implemented, approved by the PIC and published on the enterprise's website.
Means for remediation and external enforcement	
	If cause to believe that a confidentiality incident involving personal information has occurred exists, then reasonable measures to reduce the risk of injury and prevent new incidents of the same nature must be taken. - If the incident presents risk of serious injury, the following must be notified: - CAI - Person whose personal information is concerned - Any person or body that could reduce the risk may also be notified - In assessing the risk of injury, the following must be considered: - Sensitivity of the information concerned - Anticipated consequences of its use - Likelihood that information will be used for injurious purpose - Register of confidentiality incidents must be kept "Confidentiality incident" means: - Access not authorized by law to personal information, - Use not authorized by law of personal information, - Communication not authorized by law of personal information, or - Loss of personal information or any other breach in the protection of such information

As the above chart shows, the proposed legislation does not address all of the 2009 Essential Elements of Accountability, does not attempt to modernize the 2009 Essential Elements of Accountability, and for

the private sector, to a certain extent, duplicates the Digital Privacy Act amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA)[8] which introduced a mandatory data breach notification requirement

Modernizing Accountability for Quebec's Digital Future

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 technologies, including threats to the safety of personal data and to individual privacy.[9] In order for Quebeckers to benefit from this data driven age, Quebec needs an accountability framework that addresses and anticipates the benefits and detriments of digital technologies, especially those that operate without human involvement. This framework is known as Fair Processing Demonstrable Accountability which, among its requirements, includes an assessment process that balances the risk of harm and benefits to people of digital technologies. Digital technologies are electronic tools, systems, device and resources that generate, store or process data.[10] The IAF's work in Canada and other jurisdictions considers how the Essential Elements of Accountability might be updated for today's highly connected world. This work was featured in the Enhanced Data Stewardship EDIA project in partnership with the Privacy Commissioner of Hong Kong.[11] The IAF will be publishing further updated elements to address the elements of Fair Processing Demonstrable Accountability later in 2020. However, a summary version of these appears below. In short, , the accountability provisions of the proposed legislation do not come close to the requirements of Fair Processing Demonstrable Accountability. The accountability provisions of the proposed legislation provide a level of detail that does not address advances in technology, does not address the oversight and remediation necessary to make accountability successful and trusted, and take a narrow view of the scope of accountability.

For example, demonstrable accountability elements for a digital age 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

[8] https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html
[9] 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
[10] Education & Training, State Government of Victoria, Australia 2019
[11] 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

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.
- 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 does or may impact people in a significant manner.

The failure of the proposed legislation to address any of these elements of demonstrable accountability for digital technologies means that the proposed legislation is outdated before it is even passed. The proposed legislation is asking both the public and private sectors to use scarce resources to put in place processes that do not address the digital challenges of today and the future.

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

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 collect, use and disclose an individual's personal information, subject to certain exceptions. When PIPEDA was adopted, interactions with businesses were generally predictable, transparent and bidirectional. 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.[12] Given the recognition that business relationships are no longer just bidirectional and that consent may no longer always be practicable, it is outdated to draft legislation that is supposed to be modernizing to require consent as a condition to collect personal information from the individual.

Arguing that personal information may also be collected from a third person if there is a serious and legitimate reason does not work because either of the following conditions must be fulfilled: (1) the information is collected in the interest of the person concerned and cannot be collected from him in due time, or (2) collection from a third person is necessary to ensure the accuracy of the information. In other words, there are only two legitimate reasons. This provision is way too limiting to be a useful legitimate interest provision.

Given that the proposed legislation appears to try and incorporate many of the elements of the EU General Data Protection Regulation ("GDPR), it would be prudent to also incorporate the legitimacy of data processing set forth in Article 6 of the GDPR. This Article contains six legal means to process data, one of which is legitimate interests. Legitimate interest in the GDPR is much broader than legitimate reason in the proposed legislation. 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."[13] 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.[14] 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.[15] How legitimate interests is approached in the GDPR demonstrates how narrow, unworkable and outdated legitimate reason is in the Quebec proposed legislation.

Equivalency of Legal Protections is Not the Right Structure for Transfers of Personal Information

The proposed legislation provides that before communicating personal information outside Quebec, an assessment of privacy-related factors must be conducted taking into account:

1. The sensitivity of the information;
2. The purposes for which it is to be used;
3. The protection measures that would apply to it; and
4. The legal framework applicable in the State in which the information would be communicated, including the legal framework's degree of equivalency with the personal information protection principles applicable in Quebec.

[12] 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
[13] GDPR Article 6(e)
[14] GDPR Recitals 47 and 48
[15] GDPR Recital 47

The information may be communicated if the assessment establishes that it would receive protection equivalent to that afforded under the proposed legislation.[16] If this standard is not met, no transfer is allowed. Such a limited transfer mechanism is economically unviable, is destructive to businesses located in Quebec and to Quebec's economy in general, is isolationistic, and is not the kind of modernization called for by this proposed legislation.

This proposed legislation is intended to regulate both the private and public sector's communication of personal information in Quebec and personal information that has its origin in Quebec but might be communicated in another jurisdiction. Achieving domain over data through time and space has been a dilemma since the first privacy law. Canada has chosen to regulate privacy in a federal manner with oversight and enforcement duties shared between the federal government and the provinces. Just as in Europe, this approach means all jurisdictions that are party to the system are considered competent to fulfill their respective role. The proposed legislation, and its requirement for equivalent protections in other jurisdictions, does not make it clear that other Canadian jurisdictions, by membership in this federal system, are competent and therefore equivalent. If that is not the case, it has practical implications for how businesses operate. For example, it would be unfortunate if a supervisor would not have the data to oversee an employee in Quebec because his or her Canadian province had a law that accomplishes similar objectives but was not equivalent in structure.

The same could be said for transfers beyond Quebec. Many Quebeckers conduct business in other countries. Many are employed by companies in the United States, for example. In 2019, of Quebec's exports, 71.2% went to the United States.[17] Equivalency (under the name adequacy but defined as equivalency) for transfers has been built into the European private sector privacy law, the GDPR. However, Europe has only been able to find a handful of jurisdictions as adequate, and all are up for review by the European Commission. Fortunately, the GDPR allows for derogations where a company can assure European data will be protected at European standards by data controllers. However, even those derogations have been brought into question because of the ability for governments to get lawful access to data. That lawful access by government is addressed in Quebec but will not be exercisable in other jurisdictions.

Accountability is the basis for transfers in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[18] and has been the basis under Canadian law. If the government has concerns about protecting Quebeckers, it would be optimal to address the requirements through an accountability mechanism.

Further, the lack of equivalency due to the question of foreign governments' use of data from the private sector based on a lawful order should be addressed by government to government discussions. Putting the burden of determining the equivalency of a legal framework "in the State in which the information would be communicated" on the private sector that must respond to a lawful order is unreasonable and untenable. Canada's current accountability principle requires organizations to be diligent when transferring data and to stay responsible for that data when doing so. The Quebec

[16] Section 17

[17] Bill 64 and The Exportation of Personal Data from Quebec: Complications in Sight, Fasken, August 17, 2020. https://www.fasken.com/en/knowledge/projet-de-loi-64/2020/08/17-the-exportation-of-personal-data-from-quebec

[18] https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

government might consider enhancing the requirements for due diligence rather than create an equivalency requirement that would be problematic.

Privacy Legislation Should Be Proportionate

In *R. v. Oakes,*[19] 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, Division II of the proposed legislation, Collection of Personal Information, is overly narrow and therefore is not carefully designed to achieve the objective in question and is not rationally connected to that objective - a privacy law suitable for the digital age. Requiring consent for the collection of personal information in the digital age, an information-based economy using computer or other technology devices as medium or communication,[20] is often impossible. Therefore, this proposed privacy law is unlikely to be effective in meeting that need.

In addition, the proposed legislation 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 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. In particular, there must be a consideration of the need of organizations to collect, use and disclose personal information. The Purpose provision of Part I of PIPEDA[21] 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

[19] [1986] 1 SCR 103. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/117/index.do
[20] Adnan Rizal Harris, Issues in Digital Era, Research Gate, December 2016 https://www.researchgate.net/publication/328528038_Issues_In_Digital_Era/link/5bd275eba6fdcc3a8da64dd4/download
[21] https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html#h-416888

> 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 collection of personal information and underemphasizes the enterprise's need to collect, use and disclose personal information in the digital age.

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 collecting, using and disclosing personal information; equivalency of legal protections is not the right governance structure for transfers – accountability is; 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,[22] it is stated under Minimizing 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 Quebec Government wants to take advantage of, it is imperative that proportionality among fundamental rights, and not proportionality within a fundamental right, is balanced. When balancing the right of privacy and the need of organizations to collect, use or disclose personal information, it is clear that the proposed legislation is not proportionate.

Concluding Remarks

Writing privacy legislation for the next generation is difficult. It must protect the full range of individual interests 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.

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