Report for the Big Data Assessment for Canadian Private Sector Organizations Project

28 February 2017

I. Background

In early 2014, IAF began the Big Data Ethics Initiative. IAF brought together numerous thought leaders, including former data protection commissioners, to discuss the issues related to trustworthy big data analytics. Based on that dialogue, IAF published "A Unified Ethical Frame for Big Data Analysis" ("Unified Ethical Frame") in October 2014.[1] IAF also organized a plenary session at the 36th International Conference of Data Protection and Privacy Commissioners on the ethical use of big data. In 2015, IAF continued the Big Data Ethics Initiative with the creation of a model assessment framework and a customized assessment framework for digital marketing.[2] That same year IAF authored a paper on how such an assessment process might be enforced by regulatory authorities with different mandates.[3] A session to explain the oversight of big data was organized by IAF as a side event at the 37th International Conference of Data Protection and Privacy Commissioners in Amsterdam in October 2015.

II. IAF Proposal

The IAF received a grant from the 2016-2017 Contributions Program of the Office of the Privacy Commissioner of Canada that was supplemented by funding from twenty (20) Canadian companies or Canadian offices of multinational companies (Participating Companies) and in-kind services from Osler, Hoskin & Harcourt LLP. The purpose of the grant was to create for the Canadian context an assessment process (Canadian Assessment Process) to determine whether big data undertakings are legal, fair and just (Canadian Assessment Project) and to identify the elements necessary for an assessment framework to fit into a code of conduct or practice that might be enforceable by Canadian governmental regulatory agencies (Code of Conduct Elements).

III. IAF Initial Assumptions

The Unified Ethical Frame, which is the basis for the Canadian Assessment Process, is grounded in part on the overriding principle of data protection as a full range of fundamental rights associated with the processing of data that pertains to individuals. The term "privacy", as it is used in this report, is broadly comparable to the term "data protection" and is not limited to individual autonomy as is often the case.

Accountability requires an organization to understand the impact of processing on individuals, even where the individual has provided consent. Accountability is not a simple balancing of the organization's interests against the rights of the individual but rather is a more dynamic distribution that balances benefits to some individual rights and interests versus risks to the interests of others. Lastly, accountability requires an organization to be able to demonstrate that its assessment and decision making processes are done with competency and integrity.

---

[1] See attachment Part A.

[2] See attachment Part B and attachment Part D.

[3] See attachment Part C.

Consistent with the concept of accountability, when an organization intends to process personal information (in the big data context or otherwise), the organization needs to make a judgement on whether the process is "legal, fair and just". Under the Unified Ethical Frame, the concept of "legal" pertains to all the requirements of the law that impact the collection, use and disclosure of personal information and other data and the rights provided to individuals in respect of their personal information. "Fair" refers to the use of data that would be considered reasonable by an individual and beneficial to the organization using such data. The concept of "just" means that data is not used in a manner where it causes inappropriate discrimination, particularly where the discrimination is in secret.

The Canadian Assessment Project tested those assumptions and linked core concepts to the requirements of Canadian law and practice.

IV. The Canadian Assessment Project

A. Process

Starting with IAF's customized assessment framework for digital marketing,[4] IAF conducted two telephone conferences and held three in-person meetings with the Participating Companies and with Adam Kardash, the Chair of the Privacy and Data Management practice at Osler, Hoskin & Harcourt LLP, and developed a draft Canadian Assessment Framework (Draft Framework).[5] Prior to the multi-stakeholder session in Toronto on 16 December 2016, IAF shared the Draft Framework with academics, civil society, and Canadian privacy regulatory authorities. The Office of the Privacy Commissioner of Canada and privacy regulatory authorities from British Columbia, Alberta, Ontario, Quebec and Newfoundland submitted comments on the Draft Framework and/or participated in the multi-stakeholder session. Representatives from academia, civil society, and the Participating Companies participated in the multi-stakeholder session on 16 December 2016 at which the Draft Framework was evaluated.[6]

B. What was Learned

The IAF team learned a great deal from the Canadian Assessment Project. The sections that follow reflect the views and insights of the many participants in the meetings to develop and give input to the Canadian Assessment Process. The IAF is a non-profit research and education organization, and it does not speak for any of the participants. However, it is the IAF's intent to reflect the participants' views as accurately as possible in this report. The Participating Companies have highly developed management programs with privacy impact assessment processes. The IAF does not know if the views of the Participating Companies are reflective of

[4] See attachment Part D.

[5] The individuals listed on Part E participated in the development of the Draft Framework and agreed to be listed in this Report.

[6] The individuals listed on Part F participated in the multi-stakeholder session.

Canadian industry in general. The civil society was recruited based on recommendations from the agencies, business and IAF's own knowledge of active Canadian organizations and academics. The regulatory authorities were the Office of the Privacy Commissioner of Canada and the provincial privacy regulatory authorities. The Canadian government (Innovation, Science and Economic Development Canada) was invited but did not attend. The IAF paid travel expenses for some participants, but no honorariums were paid. The IAF found all the participants to be highly engaged in the Project and knowledgeable.

The sections below reflect the insights the IAF gained from the meetings with Participating Companies, consultations with privacy regulatory authorities, and the multi-stakeholder discussion.

1. During the Development of the Draft Framework

a. As can be seen by the amount of involvement by the Participating Companies, two conference calls and three all-day meetings, the Participating Companies have a stated commitment to respectfully treating data in a manner that fosters innovation but at the same time mitigating the array of privacy, legal and ethical risks associated with previously unimaginable secondary uses of data. The Participating Companies made clear to the IAF that they continue to view the framework set out under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) as an effective model for organizations to respectfully treat personal information in the course of developing and offering highly innovative and valuable services, products and features. The Participating Companies believe the reason why PIPEDA continues to be successful and why PIPEDA can continue to help foster innovation is largely grounded within the following key features of its statutory framework:[7]

(i) In their view, PIPEDA balances the rights of individuals and the interests of organizations. PIPEDA's statutory framework expressly recognizes the balancing of interests that fosters the innovation that is required in today's digital economy. PIPEDA requires organizations to protect the privacy of individuals while expressly recognizing the need for organizations to process personal information. This balance is struck in the Purpose section of PIPEDA which provides: "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 information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." PIPEDA's consent and

[7] Interactive Advertising Bureau of Canada Submission in response to the Office of the Privacy Commissioner of Canada's consent and privacy discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act* (IAB Submission) Section 2. The IAB Submission very concisely summarizes the views of the Participating Companies.

accountability requirements must be interpreted and applied with PIPEDA's purpose section admonition to balance rights and interests in mind. As stated by the Federal Court of Appeal, "There are . . . two competing interests within the purpose of the PIPED Act: an individual's right to privacy on the one hand, and the commercial need for access to personal information on the other. However, there is also an express recognition, by the use of the words "reasonable purpose," "appropriate" and "in the circumstances" (repeated in subsection 5(3)), that the right of privacy is not absolute. . . . . All of this is to say that, even though Part I and Schedule 1 of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests . . . . [F]lexibility, common sense and pragmatism will best guide the Court."[8]

(ii) From their perspective, PIPEDA is principles-based, is technologically neutral and provides a pragmatic, flexible framework. PIPEDA's consent and other provisions are mainly set out in plain language as broad principles and therefore can be applied to any new technology, new application or new ecosystem that involves the processing of personal information, including "big data" processing. It is precisely because PIPEDA does not focus on any particular-type of technology or sector that it is so well-suited to address the seemingly novel privacy considerations that may be raised by new technological developments such as big data.[9]

(iii) The Participating Companies believe that under PIPEDA's accountability principle, organizations are responsible for personal information in their custody and control, and organizations must implement policies and procedures designed to ensure compliance with PIPEDA's rules that govern the entire life cycle of the organization's personal information processing. The accountability principle holds organizations responsible for their personal information practices and does so in a non-prescriptive manner that affords organizations the flexibility to tailor, adapt, and refine their privacy programs in a practical manner that is suitable to the industry sector, size of the organization, the nature of an organization's personal information practices and the organization's evolving commercial needs. Moreover, to bolster their efforts to comply with the accountability principle, organizations can choose to participate in self-regulatory regimes, agree to adhere to codes of conduct, and/or align to supplement their privacy programs with industry standards or evolving approaches to the assessment of data practices, including ethical assessments.[10]

(iv) The Participating Companies view PIPEDA's consent requirement as just one part of an organization's broader obligations under PIPEDA's accountability principle. Under PIPEDA, an organization may not collect, use or disclose personal information

[8] Id. Section 2(i).
[9] Id. Section 2(ii).
[10] Id. Section 2(iii).

in the course of its commercial activities unless it has the authority under PIPEDA in order to do so. The authority to collect, use or disclose personal information may be obtained by consent or by a prescribed exception to consent. Practically, the substantive focus of privacy management programs (and an organization's focus on the respectful treatment of data) relates mostly to an organization's personal information practices after authority for personal information processing (whether consent or otherwise) has been obtained.[11]

b. The Participating Companies also believe that PIPEDA's current consent requirement is – and can continue to be – a legally viable and practical means for organizations to collect, use and disclose personal information in today's data environment, including big data processing, for the following reasons:[12]

(i) The core elements of PIPEDA's consent requirement – as contained in Principle 4.3 of Schedule 1 to PIPEDA and the new Section 6.1 of PIPEDA – are set out in a principle-based, technologically neutral fashion. In many technology contexts, including data analytics or big data, the consent principles can continue to serve as authority for the processing of personal information by using a flexible, pragmatic and common sense approach. The concept of data analytics is not new. Data analysis is an inherent part of research and development. However, the concept of big data processing typically refers to new analytical methods applied to large unstructured data sets and is a critical part of many companies' innovation processes. The insights derived from big data analytics now being conducted by companies are leading to a profound and unprecedented level of benefits and improvements in process efficiency and convenience and an array of new product and service offerings and features.[13]

(ii) PIPEDA's consent provisions contemplate circumstances where organizations must process personal information in connection with providing a product or service offering, such as the case where data analytics is being conducted for research and development or required as part of the product and service offering. Principle 4.3.3. of PIPEDA's consent principle provides: "An organization shall not, as a condition or the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes." This consent provision embodies PIPEDA's balancing of interests by expressly recognizing that certain types of personal information processing – such as is the case with data analytics – may be inherently required for the provision of a product or service, while at the same time ensuring that privacy rights of individuals are expressed with the inclusion of specific conditions that must be satisfied. Specifically, under Principle 4.3.3, organizations

[11] Id.
[12] Id. Section 3.
[13] Id.

can require an individual to consent – within the terms and conditions for the provision of the product or service – to certain types of processing (such as data analytics) provided that (a) the organization complies with the transparency and data minimization requirements contained within the provision (both of which requirements are consistent with other PIPEDA requirements), and (b) the collection, use and disclosure in question is done for "legitimate purposes" (Legitimate Purposes Based Consent). The phrase "legitimate purposes" is not defined in PIPEDA, but it is informed by Section 5(3) of PIPEDA which provides that organizations may only collect, use and disclose personal information for a purpose that a reasonable person would consider appropriate and by the balance of rights and interests within Section 3 of PIPEDA. Organizations in all sectors have been engaging in data analytics for decades in order to conduct research and development, prevent fraud, secure systems, and operate and provide products and services. To bolster their ability to maintain that particular types of big data processing of personal information is "reasonable", "legitimate", and "appropriate" (and their ability to rely on Principle 4.3.3), organizations can conduct these activities within their privacy management programs which include conducting assessments of the particular data practices involved.[14]

c. The Participating Companies felt that the Canadian Assessment Framework should be able to be used in a highly tailored, flexible manner, either as part of or separate from an organization's existing Privacy Impact Assessment (PIA) process. The Canadian Assessment Process does not replace the PIA process, and organizations should attempt to reduce duplication between processes. A triage approach should be used to determine whether an entire assessment needs to be done, or if, for example, because an activity is unchanged, no assessment is necessary, or because personal information is being used consistent with privacy notices and context, a PIA might be all that is needed. The Canadian Assessment Framework should be used as big data activities reach key milestones or decision points. Big data analytics often include phases (e.g., conception, approval, implementation, and review), and parts of the PIA (or specific questions within the PIA) need not be repeated in later phases if underlying conditions have not changed, but if there have been changes that might impact answers to certain questions about the data processing, then those parts of the PIA (or specific questions within the PIA) may need to be repeated. Likewise, as new data analytics and new applications of insights can change over time, the process of assessing benefits and risks may need to be repeated.

d. The Participating Companies, for the most part, felt the Questionnaire part of the Canadian Assessment Framework should be divided into two sections: Introductory Elements and Big Data Elements. Originally these elements were not separate in the Questionnaire which follows a PIA format, but the Participating Companies pointed out that they might incorporate the Questionnaire into their existing assessment

[14] Id.

processes.[15] Therefore, it was helpful to identify which elements were unique to a big data assessment and which questions needed to be asked as part of a big data assessment but might already be covered in existing PIAs. The Introductory and Big Data Elements do not constitute a complete assessment, and other elements are necessary (e.g., security safeguards and records management) for the composition of a complete assessment process. The Questionnaire has been drafted so that organizations will have options as they develop their own assessment processes. The extent to which the Questionnaire is incorporated into existing assessment processes will depend on the prior experience of the organization, previous knowledge of the organization's stakeholders, the nature of the big data activity, and the type of data involved. While all questions may not be incorporated into an organization's assessment process, it is expected that an organization will be able to demonstrate that all of the five key Unified Ethical Frame values – Beneficial, Progressive, Sustainable, Respectful and Fair – were considered as part of the assessment process.

2 During the Multi-Stakeholder Session

The tone of the Multi-Stakeholder Session was very constructive. Several topics were discussed:

a. One of the issues raised during the Multi-Stakeholder Session is whether the obligations of legal, fair and just apply to both the "thinking with data" and the "acting with data" phases of data analytics. Generally, "thinking with data" is where new insights, which go beyond experience and intuition and come instead from correlations among data sets, are discovered. "Acting with data," generally, is where these insights are put into effect and where individuals may be affected as these insights are employed in an individually unique manner. The "acting with data" phase often may be individually impactful. Many of the participants, from both the privacy regulatory authorities and civil society, were concerned with inaccurate or "false" insights coming from the "thinking with data" phase. Some were concerned with the mere presence of such insights. Others were concerned that the assessment process would reject those insights before they were used in the "acting with data" phase. There was general agreement that insights should be fully tested before being implemented. Regardless, the obligations of legal, fair and just apply to both the "thinking" and the "acting" with data phases of data analytics.

b. There was considerable discussion about the Draft Framework appropriately reflecting the balancing of interests set out under PIPEDA. Some participants felt that there is a difference between "rights" and "interests" and that the interests of individuals should

[15] The IAF believes that in a family of assessment processes based on a triage process that identifies the complexity and risks associated with a processing. PIAs historically are linked to Fair Information Practice Principles (FIPPs). The Canadian Assessment Process goes beyond FIPPs to look at the full range of rights, freedoms and interests. It is therefore a comprehensive assessment rather than a traditional PIA.

be referred to as "rights". The final version of the Canadian Assessment Framework has been drafted with the intention of clarifying that PIPEDA's purpose of attempting to reconcile many competing or complementary interests – the individual's right to privacy, other individual and societal rights and the commercial need for access to personal information – is incorporated into the Canadian Assessment Process.

c. A concern was expressed about whether the balancing being conducted during the Canadian Assessment Process is, in fact, a balancing test. This assessment process is not a scale, a teeter-totter or a seesaw. No score is generated that makes decisions for users.[16] Rather, the assessment process identifies key issues that decision makers in organizations may consider. If decision makers take into account what they learn from the assessment process, decisions may be made in a manner that gives weight to the interests of other parties but recognizes that the rights of those individuals who will be impacted by the data analysis have priority. When determining whether big data activities achieve the ethical goals of legal, fair and just, the individual's rights are paramount to the interests of the organization.

d. Some participants from civil society pointed out that the Canadian Assessment Framework is an *ex parte* application of an ethical assessment process because it is conducted completely within the organization and therefore is unlike the ethical review board process which requires participation by independent, outside experts. They therefore questioned the applicability of the term "ethics" in connection with this process. Other participants were less concerned with the term "ethics" and were more concerned with ensuring that their internal assessment processes for big data initiatives included ethical considerations regarding the use of the data in question.

e. Some of the provincial privacy regulatory authorities were concerned that individual participation through consent based on notice that triggers investigations is limited in the big data environment. This may be a particular problem in Quebec (which made comments but did not participate in the Multi-Stakeholder Session). This issue is reflected in the strong desire by privacy regulatory authorities for an appropriate oversight process.

f. The privacy regulatory authorities discussed whether this assessment process for the private sector may be appropriate for the public sector. Since the public sector is covered by a different set of laws, the privacy regulatory authorities decided to continue this discussion at a future meeting of their respective offices.

g. Unanimously, participating privacy regulatory authorities thought oversight of the Canadian Assessment Process was an issue that needed exploring. They were joined in

[16] A number of organizations have approached the IAF about creating automated assessment processes based on the framework developed here. While IAF staff view an automated process as possible, the technical skills to do so go beyond our shared competencies.

that view by civil society participants. However, many responsible businesses are concerned that oversight will be costly, not scalable, create new liability, and impact confidentiality. Also, many businesses feel additional oversight is unnecessary. Oversight comes in many forms and may include a mixture of internal and external review. However, a full discussion of oversight is beyond the scope of the Canadian Assessment Project.[17]

C. The Canadian Assessment Framework

The Canadian Assessment Framework consists of two parts: a preamble and a questionnaire.

1. The Preamble

First, the preamble discusses the need for a Canadian Assessment Process – assisting organizations leverage the potential of big data in a manner that is consistent with Canadian law while protecting individuals from the risks of both using and not using data - and how PIPEDA (and private sector and health sector privacy laws) support a Canadian Assessment Process.

Next, the preamble describes how big data analytics can be separated into the two phases of "thinking" and "acting" with data, articulates the Unified Ethical Framework's five values – Beneficial, Progressive, Sustainable, Respectful and Fair – for determining whether particular types of data analytics are legal, fair and just, and shows that consideration of these five values enhances an organization's management program and its compliance with its accountability obligations under PIPEDA. By providing a framework for establishing that the purpose and nature of big data analytics are reasonable, legitimate and appropriate in a given set of circumstances, the assessment process helps an organization, as part of its privacy management program, determine whether its big data activities are legal, fair and just and demonstrate how that determination was reached. This part of the preamble also establishes that the five values are well-grounded in Canadian law.

Finally, the preamble discusses how the Canadian Assessment Framework may be used. It should be used in conjunction with PIAs, but it is broader in scope than the typical PIA process, looking to the full range of individual rights and societal interests. For example, all data, not just personal information, are considered in this assessment process. Therefore, all aspects of this assessment process include data in the aggregate, non-identifiable form that therefore are outside the scope of PIPEDA. However, to the extent an assessment process can be used to consider and appropriately mitigate the impact of a personal information practice, such a process may supplement (or be woven into) the organization's assessment process.

[17] IAF has submitted a proposal as part of the 2017-2018 Contributions Program to conduct a dialog as a prerequisite to developing assessment framework oversight models that are trustworthy and scalable. See part III.D. *infra*.

2. The Questionnaire

Each section contains Factors for Consideration and sample Questions. The Factors for Consideration help explain the concepts and define the terms used in the sample Questions. The sample Questions help evaluate whether based on the assessment the activity is reasonable, appropriate and legitimate.

The Questionnaire generally follows a PIA format and is divided into two sections: Introductory Elements and the Big Data Elements. The Questionnaire does not constitute a complete PIA. Other elements (e.g., security safeguards and records management) are necessary for the composition of a complete PIA process.

The Introductory Elements consist of one section, Characterizing the Activity, which contains the following subsections: Accountability, Purpose, Data, Sources, Preparation, Contractual and Legal Conditions, Accuracy. The Big Data Elements consist of three sections: Characterizing the Activity, Assessment and Decision, and the Characterizing the Activity section contains the following subsections: Purpose, Insights, Preparation, Accuracy, Impacted Parties; the Assessment section contains the following subsections: Impacted Parties, Outputs, Benefits and Impacts, Risks and Mitigation, Weighing of Benefits and Risks; the Decision section contains one subsection: Overall Evaluation.

Use of the Canadian Assessment Framework helps determines whether the decisions reached on the appropriateness of an activity were well reasoned and can demonstrate how that determination was reached.

D. Going Forward

The IAF has a commitment to socialize the Canadian assessment process. Sessions have been scheduled for various Information Association of Privacy Professional events in the United States and Canada. The IAF will seek other venues for education and feedback.

The IAF considers all processes open for improvement. The current version of the Canadian Assessment Framework carries a date. As the IAF learns more, the current version will be updated and will carry a new date stamp.

Assessment processes such as this one will only be successful if they are trustworthy, i.e., these assessment processes must be demonstrable and overseen. Currently, no consensus exists on how this demonstration and oversight might take place, and there are differing views from the various stakeholders. The IAF believes a structured dialog should take place, and for this reason, IAF has submitted a proposal for funding under the Office of the Privacy Commissioner of Canada's 2017-2018 Contributions Program.

V. Code of Conduct Elements

A. Code of Conduct

In the enforcement paper issued in 2015,[18] IAF articulated, the elements of a big data code of conduct that would be subject to regulatory oversight: internal policy that mandates assessments and their integration in internal governance; assessment tool that contains the elements of the assessment framework; decision, mitigations and evidence used to make those conclusions; internal oversight over the big data process; standing ready to demonstrate the process. Fundamentally, a code of conduct is an organization's internal policy mandate that involves an assessment process. It comprises an organization's mechanism for demonstrating its process to assess the full set of risks associated with big data processing, its strategy to mitigate those risks, the basis for arriving at those decisions, its review to determine whether its risk mitigation is effective and ongoing internal oversight. The assessment framework, a data protection impact assessment customized for big data, is the mechanism for the demonstration.

The Canadian Assessment Process when implemented is the manifestation of an internal policy mandating assessments and its integration into internal governance; constitutes the assessment tool that contains the elements of the assessment framework; requires decisions, mitigations and evidence used to make conclusions; constitutes internal oversight over the big data process; is the manifestation that the organization stands ready to demonstrate the process. Thus, the Canadian Assessment Framework contains all the elements of a big data code of conduct as articulated in the IAF's 2015 enforcement paper.

[18] See attachment Part D.