IAF Consultation Contribution: “Consent and Privacy”

July 2016
IAF response to the “Consent and Privacy” consultation initiated by the Office of the Privacy Commissioner of Canada

Overview

The following comments by The Information Accountability Foundation (“IAF”) are in response to the “Notice of Consultation and Call for Submissions: Consent Discussion Paper”. The IAF is a tax-exempt, non-profit organization under Section 501(c)(3) of the United States Internal Revenue Code. It is organized and operated exclusively for research and educational charitable purposes. The IAF was formed to develop accountability-based information policy guidance that would protect individual interests while facilitating information driven innovation. The IAF team that worked on these comments was Martin Abrams, Peter Cullen, Lynn Goldstein and Nick Warren.¹ These comments reflect their views and do not necessarily reflect the views of the IAF board, funders and other participants in IAF activities.

Having read and understood the consultation procedures outlined by the Office of the Privacy Commissioner of Canada (“OPC”), we submit our comments, which relate to the following three questions in the consultation:

1. Of the solutions identified in this paper, which one(s) has/have the most merit and why?
2. What solutions have we not identified that would be helpful in addressing consent challenges and why?
3. What roles, responsibilities and authorities should the parties responsible for promoting the development and adoption of solutions have to produce the most effect system?

Question four goes beyond IAF’s charitable mission.

IAF’s comments address several actors, including industry, regulators and policymakers.

The IAF is also leading a Canadian project to develop an assessment framework for big data and similar processing that is relevant to this consultation; however, it will not be complete within the consultation time frame.

Contact and Category Information

Contact: Martin Abrams
Executive Director
The Information Accountability Foundation
mabrams@informationaccountability.org

Category: Independent Research and Educational Non-Profit Organization

---

¹ The pronouns “we” and “our” refers to the IAF staff that prepared these comments
**Comments Summary**

We believe the Office of the Privacy Commissioner of Canada has done an excellent job of presenting the current data environment and has asked appropriate questions. However, we believe there are related issues that should be raised and discussed as part of the Canadian process. Those issues include:

- Privacy law encompasses both assuring individual autonomy and fair processing of data. The two pillars of PIPEDA, consent and accountability, facilitate those two key objectives. However, emerging data ecosystems mean greater reliance on fair processing supported by accountability.
- Thinking with data and acting with data have different impacts on individuals, and guidance should differentiate the two.
- Not all data originates in the same manner. Some data is provided directly by individuals; other data is observed. In addition, some data is created as part of analytics. Policy guidance should reflect the nature of data origination and how it is classified.
- Data increasingly exists in eco-systems with many players, all with obligations to the individuals impacted by data.
- The use of ethics in assessment processes requires the privacy community to define the key ethics that need to be considered in such assessments.

We addressed a number of the solutions suggested by the consultation paper. First, we agree there are no silver bullets, and a mixture of solutions is necessary. Our other comments included:

- Transparency should be considered more broadly then just privacy notices and their functionality as it relates to consent. Transparency needs to take into consideration the audience and the purposes for informing.
- De-identification requires the belt and suspenders of technology and policy enforcement. Furthermore, there are emerging technologies that will provide more granular controls so that policy rules may be enforced with greater assurance.
- No-go zones are best guided by societal norms established by other legal regimes, such as those established for consumer and patient protection. No-go zones may have unintended consequences when thinking with data.
- We believe that ethical assessments are a natural augmentation of accountability guidance and, when used in a reasonable and legitimate manor, create something equivalent to the European concept of legitimate interests. Furthermore, ethical assessments may be supported by codes of conduct and certifications on a voluntary basis.
The Information Accountability Foundation is a tax-exempt, non-profit organization under Section 501(c)(3) of the United States Internal Revenue Code. It is currently the organizer of and secretariat for a project in Canada developing a process for ethically assessing non-traditional uses of data, while still maintaining protection and respect for fundamental rights. In addition, the IAF is leading a research initiative called the Effective Data Protection Governance project (“EDPG”), which seeks to improve operational efficiency and regulatory certainty in the digital age. While both projects are still in progress, many of the concepts illuminated by the projects are included in these comments.

Excellent Starting Point

The Office of the Privacy Commissioner of Canada has done an excellent job of framing the issues and proposing possible solutions in “Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronics Documents Act (‘PIPEDA’)”. The paper’s discussion of the challenges raised by observational data, big data, the Internet of Things and the difficulties they create for individual control are to the point and highly relevant, as are the descriptions of proposed solutions from organizations such as the IAF, Centre for Information Policy Leadership and Future of Privacy Forum. In addition, the paper highlights the need to think more broadly about organizational accountability, also a PIPEDA bedrock. The IAF has shared the OPC paper in numerous settings and commissioned a Spanish translation of the document, which will be distributed to global dialogues in which the IAF participates.

Our comments both respond to some of the solutions suggested by the paper and raise a number of side issues we believe should be part of this consultation. These additional considerations in no way impact our belief that the OPC consultation paper is an excellent contribution to improving the state of data protection.

Key Issues

Privacy Law Encompasses both Assuring Individual Autonomy and Fair Processing of Data

The Personal Information Protection and Electronic Documents Act (“PIPEDA”), provincial laws and the OECD Guidelines that form the basis for Canadian privacy law have been designed to facilitate the free movement of data and protect individuals from loss of autonomy and the negative impacts of unfair processing. There are times where

---

2 Project funding includes a research grant from the Office of the Privacy Commissioner that is being conducted with complete independence. The project will include a multi-stakeholder evaluation session that will include Canadian civil society and academic community.

assuring autonomy and fair processing are the same or similar activities. This is typically where data is provided directly by the individual and uses are easy to describe and easy to understand. As some commentators would suggest, one provides fair processing by first providing autonomy, and the best means for providing autonomy is through fully informed consent. However, sometimes what is effective in protecting autonomy does not always provide robust protections for assuring fair processing. As data becomes more robust and uses become more diverse, robust accountability may be more effective in assuring fair processing. When one thinks with data, for example, even when the data was collected pursuant to a notice that mentions research uses, assessments and mitigations as part of accountability provide the most effective elements for protection.

This consultation was begun, in part, because it is recognized that consent is not always fully effective in providing the authority for fair processing in an increasingly complex data world. To facilitate discussion, we believe it is useful to remind participants that privacy law serves the dual purpose of providing fair processing as well as autonomy. Effective fair processing requires an acknowledgment that the methodologies for providing fair processing, in some cases, deviate from or require an alternative to the best methods for providing autonomy.

Differentiating Thinking and Acting with Data

The 2013 paper “Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance”\textsuperscript{4} suggests that one differentiates the process of discovering new insights through advanced analytics, called the “discovery phase”, and applying those insights as one makes decisions, called the “application phase”. The discovery phase is typically where information driven innovation takes place. It is also a phase where there is typically less or no impact on the individuals to whom the data pertains—as long as the processing is conducted with appropriate levels of security and other obligations related to risk are met. Consent may be implied for data use in the discovery phase, but the specific research objectives are often not noted in a stated privacy policy. Therefore, an assessment processes at this stage may require additional assurance that the processing would be deemed appropriate to a reasonable individual.

The application phase is where data may be personally impactful, so governance and accountability take on greater importance. Furthermore, it is much easier to apply fair information practices such as consent when applying a model. The purposes are

generally well defined, and the data processed to achieve the purposes are clear, so privacy notices may explicitly define the activity.

For example, cardiologists have developed algorithms based on millions of past patients that predict the likelihood an individual may have a heart incident over a three-year period. The use of the data from past patients is not generally impactful on those past patients. While the past patients might not have anticipated this specific research activity going forward, they most likely would consider the research reasonable. Moreover, there are many societal benefits in this scenario that should also be factored in. The creation of the predictive model is discovery.

The model may then be used to generate scores for new patients based on their current data and used in clinical diagnosis. The scores may also be used for other less individually impactful goals (for example, allocation of health resources). The generation and use of the score is the application phase and may have impact on those patients lives. While this processing is impactful, it is an example where additional consent may be appropriate, since the purpose of processing is now known.

Discovery—where data is not personally impactful—therefore, raises less explicit harmful risks for individuals. Application—where the risks from inaccurate insights, incomplete data and discrimination are highest—is also where fair information practice risk abatements are easier to apply but also where accountability for fair processing is needed. Explicit consent, for example, is much easier to exercise and more effective and relevant when applying data when it has an individual impact rather than using data as part of discovery.

In 2015, the IAF began to simplify the terminology around these concepts: “discovery” became “thinking with data” and “application” became “acting with data”. The IAF believes that using these concepts of thinking and acting with data in developing solutions for the limitations of consent would be most useful. The IAF’s explicit recommendation is that OPC recommended practices should take this differentiation into consideration.

**Data Classification**

Privacy law typically discusses data collection but not necessarily the means by which that data is collected. The Merriam Webster definition of collection is “the act or process of getting things from different places and bringing those things together.” The place from which that data comes from is a very important consideration in governing

---

5 PIPEDA does not define collection. The Ontario law that governs the privacy of health data, PHIPA, defines collect, in relation to personal health information, to mean to gather, acquire, receive, or obtain the information by any means from any source and “collection” has a corresponding meaning.
privacy. This is recognized in the OPC paper, particularly the section on the Internet of Things.

The IAF suggests that the means by which the data is made available is also quite important. The IAF created a data taxonomy based on origin in 2014. The taxonomy described four major data classifications and raises governance issues related to each classification. The fourth classification, “inferred data”, is data created as part of the analytics process. For example, cardiologists run data from many different diagnostic tests and patient data (such as age) and come up with a calcium score that predicts the likelihood of a patient having a cardiac event over the next three years. The individual almost assuredly received notice and provided consent when he or she helped fill out the patient record or submitted him/herself to the diagnostic test. Those notices may have referred to future applications of that data. However, the analytics driven by the data that created the score is probably the most impactful piece of data of all. That most impactful data was not collected but rather was created.

The IAF believes the policy community should recognize the differences between classes of data to best design the solutions where not only the use of the data, but also, the nature of the data itself require new governance approaches.

**Data Increasingly Exists in Eco-Systems Rather than Linear Plains**

Smart phones, with their sensors and apps, began to make us aware that data no longer exist in a linear chain easily governed by accountability requirements. Instead, data exists in eco-systems that are defined by many players observing behaviour, creating data and using that data to better understand environments and create solutions. All players have obligations to the individuals impacted by the data, to other players that are part of the eco-system and to society as a whole. The IAF Effective Data Protection Governance project was created to improve understanding modern data flows, the obligations associated with uses and how they might be responsibly managed to spark innovation while protecting stakeholders. We believe the consultation paper has identified this trend; however, we believe greater emphasis would be useful when fashioning solutions.

**Defining Data Ethics**

Since 2014, the IAF has argued that fair processing involving big data analytics and complex information ecosystems requires an ethical overlay to assessing whether a processing is legal, fair and just. At the same time, privacy enforcement agencies began to suggest controllers look beyond technical compliance to ethics to evaluate whether their processing of data meets the spirit of privacy law. However, while the IAF argued

---

in favour of ethics, there has yet to be a real debate on the ethic or ethics that create
guard rails for assessments.

As a proxy for ethics, the IAF put forth five values for analysis that funnelled the decision
into a determination of what would be considered fair. When one reverse engineers
the process it can be seen that weight was placed on the following key concepts:

- Honouring commitments and established rules;
- Identifying and understanding the stakeholders, the risks they would bear and
  the benefits they might receive from the processing;
- Ensure the risks and benefits are matched to all stakeholders.

Underlying the analysis is the western ethic commonly known as the “golden rule”—do
unto others as you would have them do unto you.

The European Data Protection Supervisor (“EDPS”) recognized this definitional gap and
named an ethics advisory board to report out later this year. This board’s work will lead
to international consultations that may be helpful in creating a consensus on the key
ethics for assessing fair processing when data is used beyond the clear understandings
of individuals.

In the interim, what is left is the primacy of individual autonomy, the one key
information policy ethic that has been defined. This ethic’s influence on the
consultation is clear in the early reference to Alan Westin’s work on the importance of
consent. But if autonomy is the only ethic, then ethics do not help in resolving how to
govern when consent is not fully effective. Hence, the need for the key work mentioned
above.

We would never suggest that the IAF is the appropriate body for defining the key ethics
for this information age, but we do suggest the OPC monitor the work on defining the
key ethics of an information age being conducted by the EDPS and others. If the work
has value, it should be included in the guidance to be developed by the OPC.

**Solutions**

We first and foremost agree that the governance challenges in 2016 do not have a single silver
bullet solution. Achieving protection while facilitating data driven innovation requires a full
quiver of solutions. The IAF believes the solutions it discusses have application whether the
Canadian civil community decides legislation is necessary or not.

**Better Informed Individual Decisions**

The IAF believes that that transparency about data creation, collection, use and
management should be improved. This begins with encouragement of data users in all
sectors to test and perfect any means that helps individuals and communities of
individuals to understand data and its application. Individuals have a role in governance, through the choices they make, not only through consents, but also in with whom they do business. Groups of individuals also have a role in the pressure they bring on organizations to have data application practices that are fair and make sense. Regulators obviously have a role that is informed by the privacy policies organizations publish.

The discussion on complete versus easy to comprehend privacy notices are in many ways the wrong discussion. The IAF’s work on Effective Data Protection Governance suggests that long, detailed, complete notices have a significant role. They inform experts and create a roadmap for regulatory oversight. However, they are not overly useful in informing the decisions made by individuals. Where individuals, patients and citizens are expected to make decisions, informing mechanisms specific to those choices are needed. The United States financial services model notices, while not ideal, are an example of a notification that is specific to the choices available to individuals. It does not describe all data uses, only those where the law mandates choices. General explanations of how organizations use data, what value they create with those uses, is a third version of transparency. The IAF believes a pathway forward where all three of these transparency strategies are accepted is needed, and regulators need to not only find the multiplicity of strategies fair but also encourage their creation.

**De-identification and data obscurity**

The IAF sees data obscurity as a useful mechanism for mitigating risks to individuals, particularly where the obscuring technologies are linked with a policy promise. New obscuring technologies are beginning to evolve that will create control tools that have greater granularity. However, that data has to be matched in a manner that protects the accuracy and reliability of the insights that come with thinking with data. Therefore, the IAF sees data obscurity less as an issue related to jurisdiction for regulating personal information, but as a mitigation strategy when balancing all the factors necessary to assure the accuracy of outcomes versus access controls.

A related issue is the data governance for all data that pertains to be people whether personal or not. The EDPG project is exploring governance based on a 360-degree view of data that includes collection, creation, uses by all parties and destruction. Effective governance requires understanding the risks and benefits related to data application, whether the data is identifiable or not. The comprehensive data assessments being developed in the EDPG project include a 360-degree look at data as well as the risks and benefits to all stakeholders.

**“No-Go” Zones**

Consumer, patient, citizen and employee protection laws prohibit discriminatory uses of data. This is particularly the case when organizations are acting with data. Those
societal norms should be respected by organizations processing data beyond individual expectations. However, when thinking with data, one does not always know what insights may come from the processing. Discovering a predictive pattern is not discriminatory in itself. It is typically the acting with data where people are harmed. The creation of inaccurate knowledge, which may result from big data done badly, may create risks. That is why ethical assessment processes ask questions that will identify issues related to research quality. However, just precluding an area of research seems risky as well. Therefore, the IAF suggests that policymakers be very cautious about creating no-go zones for thinking with data.

**Accountability - Legitimate business interests, ethical assessments, codes of conduct and trust marks**

The IAF believes these solution issues are all tied together. First, IAF believes that legitimate business interests are better framed as legitimate interests. In Canada, legitimate interests may be equated with the PIPEDA concept of legitimate purposes. PIPEDA Section 5(3) discusses purposes that are “appropriate” as considered by a “reasonable person”. Legitimate interests look at the full range of risks and benefits to all stakeholders, with an emphasis on individuals, to achieve the legal, fair and just processing of data in the eyes of reasonable individuals. Data in an information age should be used to enhance the full range of human interests. Suggesting the assessment is a simple fulcrum that balances business interests against the autonomy interests of the individual is suggesting that assessment leaves the full range of interests out of the equation and creates the risk that individuals and society are harmed purely because how to create the right scale is not understood.

Ethical assessments are the means for building the scale that brings in the full range of interests of all stakeholders. The IAF’s Canadian project is designed to create a model scale to give an approximation of the point where data use is legal, fair and just.

Second, the complexity of evolving information ecosystems is exploding. There are too many players for the individual to ever understand all aspects of how data is collected, used and shared. More and more data exchange is taking place, making it too much for the individual to provide effective governance across the whole ecosystem. Each participant, whether directly known to the individual or not, must be accountable for their respective obligations based on the data they collect, receive or create, how they use the data and with whom they share.

While the IAF does not believe its role is to advise on whether new legislation is necessary in Canada, we made use of numerous provisions in Canadian law, such as reasonableness, appropriateness and legitimate, to create governance structures. In developing a Canadian assessment process for when data is collected, used and disclosed in a manner that would not have been anticipated by individuals, a framework
that goes beyond fair information practice principles needs to be in place. Such an assessment process relies on key values that are grounded in Canadian law and provide the legal rigor for determining legitimate purposes based on stakeholder interests.

Finally, one is still left with the question of whether scales are calibrated correctly, used with integrity and whether organizations have the skills sets necessary to use the scale. This is where codes of conduct have utility. This also fits well with the Canadian concept of accountability. The IAF, working with regulators from Europe and South and North America, held a consultation on how one might enforce against an ethical assessment process. As part of the consultation, the use of codes of conduct that would establish not only the integrity of an assessment process, but also the governance within the assessment process, was explored. The results of that consultation were published in October 2015 as “Enforcing Big Data Assessment Processes”.7

External certification often creates greater creditability in codes of conduct. The APEC Cross Border Privacy Rules system essentially creates a code of conduct for the cross border movement of data where adherence to the code is certified by a trust agent. The IAF believes trust marks can play a similar role for organizations that want to proactively demonstrate that they are using a common scale that has been calibrated and is being used competently with integrity.

The IAF appreciates the opportunity to participate in the consultation and would be pleased to expand more fully on any of the points made in these comments.