Renewing Privacy for the Modern Digital Economy

ICTC's Submission to the Ontario Consultation on Privacy

October, 2020

Research by

The Information and Communications Technology Council

Preface

The Information and Communications Technology Council (ICTC) is a not-for-profit, national centre of expertise for strengthening Canada's digital advantage in a global economy. Through trusted research, practical policy advice, and creative capacity-building programs, ICTC fosters globally competitive Canadian industries enabled by innovative and diverse digital talent. In partnership with an expansive network of industry leaders, academic partners, and policy makers from across Canada, ICTC has empowered a robust and inclusive digital economy for over 25 years.

To cite this paper:

Davidson, R., Matthews, M. (October 2020). Renewing Privacy for the Modern Digital Economy *Information and Communications Technology Council. Canada.*

Researched and written by Rob Davidson (Director, Data Analytics) and Mairead Matthews (Research and Policy Analyst).

Table of Contents

Introduction

There has never been a more pressing time to prioritize improving our privacy law. In just a matter of weeks, COVID-19 pushed entire communities online, making things like telehealth, teleworking, and virtual learning household names and propelling recent digital trends years into the future.[1] Among other things, the pandemic has prompted the adoption of new digital tools in all areas of our lives—for our business meetings, social gatherings, doctors visits, etc.—all of which, have clear privacy implications.[2] It is in this context that the Information and Communications Technology Council welcomes the Government of Ontario's consultation on privacy law.

Home to a bourgeoning tech industry, the country's largest health[3] and education[4] sectors, and nearly 15 million Canadians[5], Ontario is a key player in Canada's *increasingly* digital economy—in which privacy law is a core pillar. When done right, privacy law can protect the fundamental rights of patients, students, and individuals and create more certainty for businesses and consumers alike. It is important to remember that privacy exists for individuals in all aspects of their lives, not just in relation to businesses when they are consumers.

Currently, public sector activity in Ontario is governed by the Ontario Freedom of Information and Privacy Act (FIPPA) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). Healthcare activity is governed by the Personal Health Information Protection Act (PHIPA); while private sector activity falls under the scope of Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA).

- The Ontario Freedom of Information and Privacy Act (FIPPA)
- The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- The Personal Health Information Protection Act (PHIPA)
- The Personal Information Protection and Electronic Documents Act (PIPEDA)

Non-commercial activity by non-profits and charities in Ontario is not covered, nor are unions or provincial political parties. Expanding the scope and application of the

legislative framework beyond the private sector and commercial organizations is a welcome goal, however, it will be important to stay mindful of the varied needs and abilities of the different types of organizations involved. A tiered system where the regulatory requirements and penalties are based on the resources and abilities of different types of organizations could help address these challenges.

Additionally, as the Ontario government considers whether to establish its own provincial privacy legislation to replace PIPEDA, and establish new provincial rules governing things like the right to erasure and competition and data portability, it will be important to maintain clear and effective coordination between the relevant parties. Clear and effective coordination between the federal and provincial governments and between the relevant privacy and commissioners, for example, can prevent conflicting or overlapping regulation, which should be avoided.

Finally, on the more specific questions and proposals, ICTC notes the following:

- For individuals to be able to make the complex assessments required to opt-in to secondary uses of their information, they need to be privacy literate. Emphasis must be placed on ensuring that individuals fully understand their rights and that companies understand their obligations (the same can be said for any changes to those rights and obligations that stem from privacy reform).
- Increased transparency on the part of organizations is needed to provide individuals more detailed, clear, and consistent information with respect to how their data is being used. For example, individuals should know when their personal information is crossing international borders and when their information is being used for AI and automated decision making.
- Policy and regulation are only as effective as their enforcement strategies. In contexts where other things like time, money, or engagement metrics are the top priority, optional and/or poorly enforced policy and regulation is easily set aside.
- Enforceable penalties must also be significant enough to act as a deterrent against non-compliance with the law. When penalties are not significant enough, some organizations may wilfully ignore compliance with the law, managing symbolic sanctions as a cost of doing business.

Proposal 01: Increased Transparency

Increased transparency for individuals, providing Ontarians with more detail about how their information is being used by businesses and organizations.

Transparency is a fundamental part of any privacy regime. It enables informed decision making (and in turn, meaningful consent) on the part of individuals and effective oversight by regulatory authorities. Importantly, clear and easy to understand privacy policies also make Canadians more willing to do business with companies that collect personal information.[6]

At a very basic level, current privacy legislation requires organizations to be transparent about what personal information they collect and how they use it, as well as what personal information they disclose to third parties. Yet, 34% of Canadians feel that they do not have enough information to know how new technologies (like AI) might affect their personal privacy, and 45% feel that businesses in general do not respect their privacy rights.[7] The Government of Canada's National Data and Digital Consultations also showed that Canadians want more transparency in how their data is collected and used.[8]

Why is there such inconsistency between *what privacy law requires and how individuals feel*? While there are many reasons for this phenomenon, several are discussed below.

The current legislative framework relies heavily on the individual's consent and places the responsibility to assess privacy risks on individuals and not organizations. This has proven overburdensome and impractical in today's complex privacy landscape, where individuals are likely to have tens, if not hundreds, of privacy policies to read each day. As individuals become less able and less likely to read privacy policies before providing consent, their consent becomes increasingly less meaningful. Measures like privacy impact assessments (PIAs) could help build upon the existing framework by putting some of the onus to assess privacy risks on

commercial organizations. To reduce the regulatory burden on commercial organizations, these kinds of measures might be required only in certain instances of data use, perhaps dependent on the sensitivity of the personal information being used. Similarly, they could be mandatory only upon request.

There is an insufficient level of detail, clarity, and consistency required by the current legislation when it comes to privacy policies. Loose requirements have resulted in misleading and confusing practices among many organizations—although this is not always purposeful. As a matter of best practice, privacy policies should not only explain *what* information is being collected, but *why* (e.g., is it for marketing purposes, for the functionality of the product or service, etc.). They should be clear, easy to understand, and easy to access, which could be ensured through universal standards governing their layout and content. Individual requests for personal information should be clearly separated from one another using opt-in interfaces, and requests should never be bundled. Privacy policies should also clearly state how the individual can withdraw their consent in the future. Finally, it is important to mention that more detail is not always better, as too much detail can overwhelm individuals, resulting in consent fatigue.[9]

Transparency requirements need to be adapted to account for modern uses of data, such as frequent cross-border data flows and the large-scale sale of personal data by digital companies and data brokers. The modern digital economy necessitates constant data flows across national borders. While current legislation requires companies and organizations to disclose to individuals whether their information will be shared with any third parties, there is no specific requirement to obtain consent for cross-border data flows.[10] At the same time, it is not always easy for individuals to determine exactly *where* their information is going. This is important for individuals to know—cross-border enforcement of domestic privacy law is not always guaranteed. The European Union's General Data Protection Regulation (GDPR) and Québec's newly proposed legislation tag additional requirements to cross-border data flows, including mandatory PIAs and equivalency requirements. While this is not the place to comment on the suitability of these kinds of requirements for Ontario, there should, at the very least, be more transparency around the use of cross-border transfers. This can also be said for the sale of personal data by companies and organizations.

Amendments need to be made to account for AI and automated decision making, which did not exist in the form that they do today when the current legislation was drafted. AI and automated decision making are central to this discussion on privacy. These topics need to be addressed so that individuals in Ontario can be certain that Ontario businesses will uphold their privacy, even in the context of new technologies and business models.

Organizations throughout Ontario are introducing AI to replace and/or supplement human decision making and analysis. At the same time, AI requires vast amounts of personal information to perform well and return promising results. For these reasons, AI is profoundly impacting the way we use personal information, both in terms of our policies and practices, and the types of activities we use personal information for.

In turn, there is an urgent need to increase transparency around the use of personal information for AI and automated decision making. It is important to stay prudent in our approach to regulating AI (and to avoid overregulation), yet an inadequate regulatory response will leave individuals without the explicit tools and levers needed to protect themselves and their personal information effectively. At the very least, the following requirements and rights are needed:

- **A requirement for organizations to proactively and responsibly disclose** the use of automated and semi-automated decision-making systems. Individuals need to be aware of—and understand the implications associated with—the intended use of their data.
- **A right for individuals to be informed** when subject to automated and semi-automated decision making.· **A right for individuals to access commercial organizations' policies and practices** for the use of personal information in automated and semi-automated decision making.· **A right for individuals to access specific information about automated and semi-automated decision-making systems**, such as the degree of human involvement in decision making; the degree of decision traceability; and key characteristics of training data, including potential biases.[11]

Proposal 02:
Enhanced Consent

Enhanced consent provisions allowing individuals to revoke consent at anytime and adopting an “opt-in” model for secondary uses of their information.

Allowing individuals to revoke consent at anytime sounds like a move in the right direction, but the details concerning how easy and enforceable the process is for individuals will determine if it is impactful or not. If individuals are forced to engage costly legal representation to force compliance, enhanced consent provisions will not have helped.

For individuals to be able to make the complex assessments required to opt-in to secondary uses of their information, they need to be privacy literate:

> *“Our data and digital world are getting ever more complex to fully comprehend and navigate, and privacy literacy training, starting perhaps early in schooling (as well as adult literacy), may better equip Canadians with the skills to engage confidently in an increasingly digital world (without compromising personal data). Tackling the demand side of the equation (consumer literacy) will be as important as building the safeguards from the supply side (industry).”*
>
> *- Namir Anani, President and CEO, ICTC [12]*

PIPEDA possesses relatively strict consent rules, whereas GDPR is more flexible. PIPEDA dictates consent as the only basis for collecting and processing personal data, whereas in the GDPR Article 6.1, there are six cases under which data can be legitimately processed, only one being via consent.

However, there is also much discussion and research concerning the appropriateness of consent-based models. Digital privacy philosopher Helen Nissenbaum argues against the basic tenants of the digital/data consent model, citing “…misimpression

of meaningful control …" and "…consent…it's simply not a measure of privacy…" as key reasons.[13] Conversely, others including responsible data veteran Alix Dunn proposes agile ethics as a model to integrate into privacy models.[14] Dunn defines agile ethics as follows: "The purpose of 'agile ethics' is to facilitate working ethically at speed, and it is a practice that can be designed to operate in tandem with agile development."[15]

Ontarians need a national data consent legislative framework to not only protect their rights but to disambiguate the differences between PIPEDA and Ontario privacy regulations – some of which can be challenging to compartmentalize. The consent framework should also be tiered, based on the relative and potential risks and harms associated with the specific categories of personal data (consumer, health, location, religion, politics, etc.), whether the data is necessary for delivering the specific service/product to the individual, and whether or not the consent request can be truly considered informed consent (according to appropriate standards or benchmarks).

From ICTC's previous submission to OPC:

Consent/no consent is a false dichotomy, there are other meaningful consent models that can be explored beyond direct individual consent. In personal finance, people can employ accountants to represent them for tax and finance preparations. For consent, there is an opportunity to create the role of a personal data protection agent, who works on behalf of individuals. To ensure satisfactory protection of personal data, these agents should be:

- Industry certified, similar to Chartered Professional Accountants;
- Required to stay up to date with all data privacy and consent developments;
- Able to provide individuals with sound advice regarding consent and meaningful consent;
- Able to act as a proxy for individuals to grant and revoke consent.

Proposal 03:
The Right to Erasure

Right for individuals to request information related to them be deleted, subject to limitations (this is otherwise known as “Erasure” or “the right to be forgotten”).

There is an argument to be made that in instances where Canadians feel their personal data has been altered, misused, or otherwise negatively impacted, they should have the right to have it lawfully erased.[16] This is especially important for minors and other vulnerable groups.

In recent letter, the Privacy Commissioner of Ontario argued that under current legislation, residents of Ontario *should* be able to request the deletion of their personal information if they did not consent to its original collection or use. However, recent events have demonstrated that, in practice, this does not always happen—consent is not always the most effective tool for deleting personal information, especially personal information that is publicly available.[17] This is because there are ambiguities in Canadian privacy law: the current definition for publicly available information may not provide enough clarity for businesses and individuals to understand how personal information in the public domain should be protected.[18]

European residents have had a basic “right to erasure” or “right to be forgotten” since 2014, reiterated in 2018 under Article 17 of the GDPR. Article 17 grants European data subjects an explicit right to be forgotten and clarifies specific timelines and processes by which this right should be met. Similarly, the California Consumer Privacy Act (CCPA) signed into law in 2018, grants residents of California the right to have their personal information deleted by businesses upon their request. Québec, in its recently proposed legislation, is also looking to implement a right to erasure in the near future.

Ultimately, the explicit rights to erasure and deletion afforded by the GDPR, CCPA, and recently proposed Québec legislation are not matched in Canadian privacy law.

Implementing a clear and explicit right to erasure for Ontarians would help solve some of the ambiguities that exist today.

That said, one important caveat of the right to erasure is that, unrestricted, it has potential to be used by bad actors and authoritarian governments to limit journalism and free speech.[19] The GDPR (in Europe) contains several measures that are purposefully designed to balance the right to erasure with freedom of expression, freedom of information, and journalistic and public interests.

Critically, a 2019 ruling by the EU's highest court found that some aspects of the right to erasure could only be enforced within the legal jurisdiction of the EU.[20] In the context of search engines that delist publicly available information from third party websites, for example, an EU resident's right to erasure would not outweigh global interests regarding freedom of information. Alongside the Charter of Rights and Freedoms, such purposefully designed mechanisms would be important caveats to any right to erasure in Canada as well.

Proposal 04:
Data Portability

Right for individuals to obtain their data in a standard and portable digital format, giving individuals greater freedom to change service providers without losing their data (this is known as “Data Portability”).

Data portability is an important and necessary part of digital governance, however, its most appropriate home in Canada may not be in privacy law. This is because data portability is not only related to privacy but also competition; it is therefore important that it be addressed with clear coordination between the relevant privacy and competition authorities. Independent pursuit of data portability by separate authorities could result in conflicting or overlapping regulation and, in turn, a greater burden to businesses and organizations.

In other jurisdictions, this distinction may not be the case. In the United States, for example, competition and privacy are regulated by the same authority (The Federal Trade Commission). In Europe, competition and privacy concerns regarding data portability are regulated under the same act (The General Data Protection Regulation). In Canada, competition and privacy law are separate. Privacy stems from the Charter of Rights and Freedoms, and it is regulated under federal and provincial privacy law and governed by the corresponding commissioners. Competition, on the other hand, is regulated under the Competition Act and the Consumer Protection Act and governed by corresponding authorities. For this reason, Canada may be better suited to a solution like Australia’s, where data portability is overseen collectively by the competition and information commissioners, despite falling under a treasury law (not a privacy law).[21]

Nonetheless, data portability has clear implications for privacy. Data portability clauses, such as that in Article 20 of the GDPR, grant individuals the right to receive their personal data in a structured, commonly used, and machine-readable format along with the right to transfer that data to another company or service provider. Data portability can urge companies to compete for individuals’ data and business, in the

interest of not losing access to valuable information in an environment where data is money.[22] To that end, data portability rights address power imbalances[23] by reducing switching costs[24] and giving individuals:

- More freedom and ability to shop around for alternative products and services;
- Greater capacity to make meaningful choices (which in turn renders their consent more meaningful); and
- More influence on the privacy practices of companies and organizations.

Presently, there is no right to data portability provided by any Canadian privacy law.[25] PIPEDA does provide individuals a right of access to their personal data (or copies of that data) held by organizations, however this right is limited. For one, it does not require organizations to give individuals *actual copies* of the data but rather simple access to the data (this could mean allowing them to view the data in an isolated instance).[26] It also does not provide individuals the right to *share or transfer their data* to other companies or service providers.

Looking forward, it will be important to secure a right to data portability for Ontarians and Canadians alike. Doing so will bring Ontario and Canada in line with international requirements under the GDPR, but it will also ensure the appropriate balance of power between consumers and companies in the digital economy. In establishing this right to data portability, there are several important considerations:

- The right to data portability should be coordinated effectively between the federal and provincial governments and between the relevant privacy and competition commissioners. Conflicting or overlapping regulation should be avoided.
- Individuals' rights to data portability need to be balanced with companies' rights to protect their intellectual property (IP). Like with the GDPR, there should be clear distinctions between personal data and the IP derived from that data.
- Standard requirements for all sectors of the digital economy can be complimented by more specific requirements in certain sectors, like healthcare or banking.

Proposal 05:
Stronger Enforcement

Increased enforcement powers for the Information and Privacy Commissioner to ensure businesses comply with the law, including the ability to impose penalties.

Across the relevant Acts, the Information and Privacy Commissioner of Ontario has very limited enforcement powers that apply to businesses. The Commissioner can impose administrative penalties of up to $100,000 on health information custodians that have contravened PHIPA and issue orders to public organizations that have contravened FIPPA, yet these enforcement powers mostly apply to public organizations, not businesses.[27]

At the federal level, the Office of the Privacy Commissioner of Canada, which oversees PIPEDA, also has limited enforcement powers. Among Canada and its trading partners, Canada's federal Privacy Commissioner is one of the only privacy authorities without the power and ability to make binding orders, proactively compel evidence of compliance, and impose consequential administrative penalties for non-compliance with the law.[28]

Policy and regulation are only as effective as their enforcement strategies. In contexts where other things like time, money, or engagement metrics are the top priority, optional and/or poorly enforced policy and regulation is easily set aside. Many businesses operate in a global economic context where vastly different and rapidly changing domestic laws and cultural norms can be overly burdensome and confusing to navigate; in this context, policy and regulation with clear and effective enforcement strategies are needed.

Enforceable penalties must also be significant enough to act as a deterrent against non-compliance with the law. When penalties are not significant enough, some organizations might wilfully ignore compliance with the law, managing symbolic sanctions as a cost of doing business. In relation to competition law, for example, the

Competition Commissioner Matthew Boswell has said that “the maximum penalties for anti-competitive behaviour […] lack the teeth necessary to deter anti-competitive behaviour.”[29] For businesses, penalties should be determined as a percentage of company revenue, with a minimum dollar amount (to be determined by the province). Many large enterprises (with billions of dollars in market cap) may simply factor in flat rate penalties as part of the cost of business.

That said, future changes to the enforcement powers of the commissioners should consider the full range of organizations that are subject to privacy law, especially if the government chooses to pursue the expansion of the scope of privacy law. A tiered enforcement system that invokes proportional sanctions for the various organizations —small, medium, and large enterprises, charities and not-for-profits, trade unions, and political parties—would be most suitable.

Proposal 06:
De-Identified and Derived Data

Introducing requirements for data that has been de-identified and derived from personal information to provide clarity of applicability of privacy protections.

De-identification and other privacy techniques like synthetic data need to be looked at from the perspective of risk management. These techniques are valid, but they are simply elements of larger risk management plans and not solutions in themselves. Risk management plans include detailed scenarios that identify the likelihood of reidentification for individuals and groups of individuals, in addition to the probable level of harm if data is reidentified. Importantly, risk management plans need to be transparent and accessible so that individuals can properly assess the risk of reidentification and meaningfully object to data collection, processing, and storage.

Similar to the EU model, reformed privacy rules and legislation should incorporate the need for a Data Protection Officer. This officer should be certified in the proper use and monitoring of emerging industry standard de-identification techniques, such as synthetic data and differential privacy.

Proposal 07: Expanding Scope

Expand the scope and application of the legislative framework beyond the private sector and commercial organizations.

Expanding the scope and application of the legislative framework beyond the private sector and commercial organizations is welcome goal, however, it needs to be done in a way that is mindful of the various types of organizations involved. It is important to remember that expanding the scope of the legislative framework will necessarily lead to increased compliance costs and new penalties.

Some organizations (small charities, not-for-profits, and unions, for example) may be hard-pressed to find the necessary resources to adapt to and comply with new legislation. For many of these organizations, fines and penalties in line with those imposed on the private sector would be overly burdensome, and this is especially true in the current economic climate. Many organizations are still adapting to new pandemic-related health and safety requirements. Meanwhile, donations to charities and not-for-profits have taken a significant hit.[30]

What would an expanded scope look like? Currently in Ontario, the legislative framework for privacy governs only the following types of entities:

- **Provincial and federally regulated organizations** that engage in commercial activity are governed by *PIPEDA;*
- **Provincial public sector organizations**, such as the provincial government, select provincial agencies, hospitals, universities and colleges are governed by *FIPPA;*
- **Municipal public sector entities**, such as municipalities, school boards, transit commissions and police service boards are governed by *MFIPPA; and*
- **Health organizations**, such as hospitals, long-term care facilities and pharmacies are governed by *PHIPA*.

By default, entities that fall outside the bounds of these four definitions are not presently regulated. This includes federally and provincially regulated organizations that are not public or health organizations and are not engaged in commercial activity. More specifically, this can include charities, not-for-profits, trade unions, and provincial political parties.[31]

Again, in expanding the scope of the current legislative framework, it will be important to stay mindful of the varied needs and abilities of the different types of organizations involved. For example, a tiered system for associated regulatory requirements and penalties could help address these challenges. Requirements and penalties would be designated based on the resources and abilities of the different types of organizations.

Proposal 08:
Data Trusts

Create a legislative framework to enable the establishment of data trusts for privacy protective data sharing.

In September 2019, the Ontario government published the second of three discussion papers focused on the province's data economy. This paper covered topics such as sharing Ontario government data and expanding digital infrastructure but neglected to discuss the pivotal need for federal, municipal, and private sector Canadian data to complement Ontario's data.[32] Unfortunately, data-sharing models tends to be pushed to the wayside or forgotten altogether.

While there is no "magic bullet" that can be applied to this data-sharing challenge, the concept of a data trust is one that can generate significant inroads and enable the innovation potential of Canadian businesses. The benefits of such a construct don't end at access. When designed and implemented properly, a data trust can balance the competing needs for responsible data access, individual and group privacy, the management of sensitive data such as medical and social services research, and the development of commercial products.

In a 2019 Open Data Institute (ODI) sponsored report, legal experts advised that traditional trust law is not a good model for data trusts.[33] Data trust regulations need to address data privacy for both individual and communities/vulnerable groups, legal responsibilities of data trustees, liability considerations for data breaches and misuse, and the rights of data subjects know and consent to the use of their data.

A further study commissioned by the ODI, *Extended ODI Data Trust report: 5*, set forward models for different data trust use cases and the structures and legal frameworks required.[34]

Conclusion

In the context of the COVID-19 pandemic, which has prompted the adoption of new digital tools in all areas of our lives, there has never been a more pressing time to prioritize the improvement of Ontario's privacy law. The above proposals could potentially serve as a guide to this legislative recalibration.

ENDNOTES

[1] Avis Favaro and Elizabeth St. Philip, "Ontario implements virtual medical visits in bid to keep doctors, patients safe amid COVID-19", March 14, 2020, CTV News, https://www.ctvnews.ca/health/coronavirus/ontario-implements-virtual-medical-visits-in-bid-to-keep-doctors-patients-safe-amid-covid-19-1.4853436; "Canadian Perspectives Survey Series", April 17, 2020, Statistics Canada, https://www150.statcan.gc.ca/n1/daily-quotidien/200417/dq200417a-eng.htm; "COVID-19: reopening schools", October 8, 2020, the Government of Ontario, https://www.ontario.ca/page/covid-19-reopening-schools#section-1
[2] Zoom, 2020, https://zoom.us/; "Houseparty is a face to face social network", 2020, Houseparty, https://houseparty.com/; "Ontario telemedicine Network", 2020, OTN, https://otn.ca/patients/evisit/
[3] Statista Research Department, "Number of hospital establishments in Canada as of 2019, by province", March 2020, Statista, https://www.statista.com/statistics/440923/total-number-of-hospital-establishments-in-canada-by-province/
[4] "Number of students in regular programs for youth", 2020, Statistics Canada, https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3710000701
[5]"Ontario Demographic Quarterly", June 23, 2020, the Government of Ontario, https://www.ontario.ca/page/ontario-demographic-quarterly-highlights-first-quarter-2020
[6] "2018-19 Survey of Canadians on Privacy", March 11, 2019, The Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/
[7] Ibid.
[8] "Strengthening Privacy for the Digital Age", May 21, 2019, the Government of Canada, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html
[9] Ibid.
[10] "Commissioner concludes consultation on transfers for processing", September 23, 2019, The Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/
[11] The degree of human involvement in decision-making: Was the decision semi- or fully automated? If there was a human involved, what was their role, and how did they rely on the decision-making system to come to their final decision? What other factors did they consider? The degree of decision traceability: How transparent is the model? Can it be explained? Are you able to trace exactly why, how, and according to what variables it makes decisions? Key characteristics of training data, including potential biases: How diverse was the data used to train the AI model? Are there any potential biases resulting from the training data? What are those biases, and how might they affect the current decision?
[12] Namir Anani, interview, ICTC CEO, October 14th , 2020
[13] BERINATO, S. (2018). STOP THINKING ABOUT CONSENT: IT ISN'T POSSIBLE AND IT ISN'T RIGHT. Harvard Business Review. Retrieved from Harvard Business Review: https://hbr.org/2018/09/stop-thinking-about-consent-itisnt-possible-and-it-isnt-right
[14] Anna Scott, A. D. (2018, 10 05). 'agile ethics', how innovative organisations can adopt them and why diversity is so important to ethics. Retrieved from Open Data Institute: https://theodi.org/article/agile-ethics-pioneer-alix-dunnon-how-to-minimise-harm-and-why-moving-fast-and-breaking-things-must-not-extend-to-ethics/
[15] Dunn, A. (2018, May 7). Working Ethically At Speed. Retrieved from Medium: https://medium.com/@alixtrot/ working-ethically-at-speed-4534358e7eed
[16] "ICTC's Perspectives on a Data Economy Strategy", November 2019, Information and Communications Technology Council, https://www.ictc-ctic.ca/wp-content/uploads/2018/11/ICTC_Whitepaper_Perspective-Data-Econ-Strat.pdf
[17] Ibid.; Mairead Matthews, "Facial Recognition Company Clearview AI Provides a Useful Case Study for the Right to be Forgotten in Canada", June 18, 2020, Digital Think Tank by ICTC, https://medium.com/digitalthinktankictc/facial-recognition-company-clearview-ai-provides-a-useful-case-study-for-the-right-to-be-forgotten-1b2584065e2e
[18] Ibid.
[19] Ibid.
[20] "Press Release No 112/19", September 24, 2019, Court of Justice of the European Union, https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190112en.pdf
[21] "Consumer data right (CDR)", September 4, 2020, Australian Competition and Consumer Commission, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/memorandum-of-understanding-with-the-office-of-the-australian-information-commissioner
[22] Ibid.
[23] Some critics have casted doubt on whether consumers will act on these freedoms and abilities in relation to privacy. Alex Marthews and Catherine Tucker, "Privacy policy and Competition", December 2019, Brookings, https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf
[24] In competition law, barriers that prevent consumers from choosing alternative products or services are referred to as switching costs. Alexandra Mitretodis and Brock Euper, "Canada: Interaction between privacy and competition law in a digital economy", August 2019, Fasken, https://www.mondaq.com/canada/antitrust-eu-competition-/832380/interaction-between-privacy-and-competition-law-in-a-digital-economy;

[25] That said, the province of Québec recently proposed new privacy legislation that would further establish and expand a person's right to access, if passed. Specifically, an individual would have the right to access computerized personal information about them in a structured, commonly used technological format; or require such information to be released to a third person. "Projet de loi no 64", June 12, 2020, National Assembly of Québec, http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html
[26] "The International Comparative Legal Guide to: Data Protection 2018", 2018, GLG, https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf
[27] That said, following recent amendments to PHIPA, some health technology companies will be considered under the scope of the Commissioner's administrative penalty and order making powers. "Startup and emerging company services/Technology, media and telecommunications bulletin", April 1 2020, Fasken, https://www.fasken.com/en/knowledge/2020/04/significant-changes-to-ontarios-health-privacy-law-technology-providers-take-note/; "Role and Mandate", 2020, Information and Privacy Commissioner of Ontario, https://www.ipc.on.ca/about-us/role-and-mandate/
[28] "2019-2020 Annual Report to Parliament on the Privacy Act and Personal Information Protection and Electronic Documents Act, 2020, Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201920/ar_201920/#heading-0-0-5
[29] "Highlights form the Competition Bureau's Data Forum", August 30, 2019, Government of Canada, https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04492.html#sec06
[30] Kate McGillivray, "1 in 5 Ontario non-profits could be forced to shut down by end of year, survey finds", August 20, 2020, CBC News, https://www.cbc.ca/news/canada/toronto/ontario-non-profits-shut-down-1.5692827; Marc Montgomery, "Canadians donating less, survey", September 17, 2020, https://www.rcinet.ca/en/2020/09/17/canadians-donating-less-due-to-covid-and-we-charity-scandal-survey/
[31] Not-for-profits, charities, and trade unions in Ontario are only subject to privacy legislation if they process personal information in relation to a "commercial activity" or if they have operations/collect information in jurisdictions that regulate these sectors, such as Alberta, British Columbia, and Québec. Similarly, they are only subject to penalties in cases where Alberta law applies, or in cases where PIPEDA applies to a data breach scenario. Miller Thomson LLP, "New privacy law could apply to all non profits", September 9, 2020, Mondaq, https://www.mondaq.com/canada/privacy-protection/983430/new-privacy-law-could-apply-to-all-non-profits-ontario-government-launches-consultations; Christopher Rootham, "A Union's Privacy Obligations", January 6, 2011,Nelligen Law, https://nelliganlaw.ca/article/labour-law/a-unions-privacy-obligations/
[32] Queen's Printer for Ontario, "Discussion paper 2: creating economic benefits", https://engage.ontario.ca/en/content/discussion-paper-2-creating-economic-benefits , September, 2019.
[33] Queen Mary University of London, BPE Solicitors LLP and Pinsent Masons LLP: "Data Trusts: what legal requirements are needed to support them?", http://theodi.org/article/data-trusts-legal-report/, The Open Data Institute, April 2019.
[34] BPE Solicitors LLP: "Extended ODI Data Trust report: 5", http://theodi.org/wp-content/uploads/2019/04/BPE_PITCH_EXTENDED_ODI-FINAL.pdf, The Open Data Institute, April, 2019.

Photographs by Matthew Henry
https://unsplash.com/@matthewhenry

The Information and Communications Technology Council

The Information and Communications Technology Council is a not-for-profit, national centre of expertise for strengthening Canada's digital advantage in a global economy. Through trusted research, practical policy advice, and creative capacity-building programs, ICTC fosters globally competitive Canadian industries enabled by innovative and diverse digital talent. In partnership with an expansive network of industry leaders, academic partners, and policy makers from across Canada, ICTC has empowered a robust and inclusive digital economy for over 25 years.

www.ictc-ctic.ca