Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

OPEN LETTER

October 16, 2020

The Hon. Lisa M. Thompson
Minister, Ministry of Government and Consumer Services
College Park, 5th Floor, 777 Bay Street
Toronto, Ontario
M7A 2J3

Dear Minister Thompson:

Re: *Ontario Private Sector Privacy Reform* Discussion Paper

On behalf of the Office of the Information and Privacy Commissioner of Ontario (IPC), thank you for the opportunity to provide our views on the Ontario government's Discussion Paper, *Improving private sector privacy for Ontarians in a digital age* (the Discussion Paper). I commend the government for taking on this important initiative. The time has come for Ontario to fill important gaps in its existing legislative frameworks and integrate privacy protection across its public, private and health sectors. The opportunity is now to address the increasingly digital landscape through the creation of a modern, made-in-Ontario private sector privacy law that suits our province's culture, values, and reality.

Given our mandate, knowledge, and experience related to data protection, we are pleased to offer our advice and assistance as the government explores the path forward. The release of the Discussion Paper with an invitation for public and stakeholder engagement is an essential first step in gathering input.

Attached are my office's initial comments in response to the issues raised in the Discussion Paper. As specifics become available, my office remains committed to working collaboratively with the government on further reflection of a "next-generation" private sector privacy law for Ontario.

In the spirit of transparency, this letter and attachment will be posted on our website.

Sincerely,

Patricia Kosseim
Commissioner

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel/Tél: (416) 326-3333
1 (800) 387-0073
Fax/Téléc: (416) 325-9195
TTY/ATS: (416) 325-7539
Web: www.ipc.on.ca

IPC Comments on the Ontario Government's Discussion Paper:
"Ontario Private Sector Privacy Reform:
Improving private sector privacy for Ontarians in a digital age"

Table of Contents

DESIGNING A MODERN PRIVACY FRAMEWORK

A. Introduction

The Information and Privacy Commissioner of Ontario (IPC) is pleased to file this submission in response to the government's call for comments on its August 13, 2020 Discussion Paper, "*Ontario Private Sector Privacy Reform: Improving private sector privacy for Ontarians in a digital age*" (the Discussion Paper).[1] We applaud the government for initiating such an important dialogue, especially during this critical time.

1. A time of mounting urgency

The mounting pressures for a made-in-Ontario private sector privacy law have become even more urgent in the current COVID-19 context. Consumers are now, more than ever, vulnerable to privacy and security risks as they carry out most of their lives online to heed social distancing warnings. This includes working remotely, following on-line classes, attending virtual health appointments and socializing with their friends using social networking platforms. For example,

[1] Ontario Government, "Ontario Private Sector Privacy Reform: Improving private sector privacy for Ontarians in a digital age" (13 August 2020), retrieved on September 28, 2020.

according to Statistics Canada, e-commerce retail sales had already surged by almost 100% from February to May 2020[2] and telework capacity has been estimated to accommodate up to 85% of the workforce in some sectors, and much less so in others, having potentially disproportionate impacts with "far-reaching social and economic implications".[3]

For their part, businesses are under pressure like never before as they try to pivot quickly from established practices to develop new products and solutions and find more flexible ways of delivering their services. A McKinsey study shows that the rate of business digital adoption accelerated five years forward in just eight weeks following the onset of COVID-19.[4]

Governments recognize the importance of reaching out across traditional lines and silos and enabling cooperation with private sector organizations to help solve some of the most vexing economic, health, and social problems the world has seen in decades. The collaboration among the Federal Government, provincial governments, Google, Apple, Shopify, and Blackberry that led to the successful development and launch of the COVID Alert App is an excellent example of such collaboration.[5]

2. Privacy as an enabler

Consumers, businesses, and governments have all come to the shared realization that privacy protection, far from impeding innovative solutions, is key to enabling their success.

To drive up adoption rates for any new product or service, consumers must fundamentally trust it. Yet, hidden consumer profiling practices, over-zealous data collection, and careless technological developments, coupled with high-profile data breaches and ransomware attacks have rattled consumers' confidence.[6] Only if people believe that their sense of privacy, autonomy and dignity is being respected and upheld will they come to trust alternate service delivery models and adopt new information technologies on offer. And only with the public's trust and willingness to embrace innovation will Ontarians' economic, health, and social well-being improve and thrive over time.

For their part, businesses and other organizations need a regulatory regime for privacy protection that is principles-based, fair and well-balanced, pragmatic, flexible, and proportionate. They need an agile and supportive regulator with modern tools to incentivize responsible innovation, not

---

[2] Statistics Canada, "Retail e-commerce and COVID-19: How online shopping opened doors while many were closing" (24 July 2020), retrieved on October 11, 2020.

[3] Statistics Canada, "Running the economy remotely: Potential for working from home during and after COVID-19", (28 May 2020), retrieved on October 13, 2020.

[4] McKinsey Digital, "The COVID-19 recovery will be digital: A plan for the first 90 days" (14 May 2020), retrieved on October 11, 2020.

[5] Ontario Government, "COVID Alert Available for Download Beginning Today" (21 July 2020), retrieved on October 11, 2020.

[6] According to a 2018-2019 national survey conducted on behalf of the Office of the Privacy Commissioner of Canada, 92% of survey participants expressed some level of concern about their privacy, and 45% did not feel that businesses generally respect their privacy rights. Eighty-eight percent (88%) of survey participants were at least somewhat concerned about organizations using their online information to make decisions about them, and 74% have not installed or have uninstalled apps because they were concerned about the personal information they were being asked to provide. Office of the Privacy Commissioner of Canada, "2018-19 Survey of Canadians on Privacy" (March 2019), retrieved on August 25, 2020.

dampen it. They need a clear framework of predictable rules that are interoperable with those of other jurisdictions in Canada and abroad. Such rules need to be enforced with due regard to procedural fairness, in a manner that rewards good behaviour and levels the playing field for all competitors in the marketplace. Without that, non-compliant organizations will continue to get away with bad behaviour, inevitably winning out at the expense of responsible organizations that expend additional resources to treat consumers respectfully and appropriately safeguard their personal information.

The Ontario government is looking to capitalize on innovative digital approaches to deliver more cost-efficient and personalized services to Ontarians.[7] Where appropriate, the government wants to work with commercial partners to realize the benefits of information technologies and alleviate costs that can no longer be sustained by the public purse alone. It wishes to attract investors and create fertile ground for developing new business models to boost the economy. To do all of this, Ontario needs a modern, comprehensive, and coherent privacy regime with an independent regulator whose oversight authority provides a one-stop-shop for resolving issues at the intersection of public, private, and health sectors interoperably with that of other jurisdictions. It also needs an effective privacy governance framework that evaluates the broader ethical considerations of using personal information, by realigning risks and benefits to protect the public interest, considering local culture and values.

3. The evolving global context

Many jurisdictions around the globe have undertaken legislative initiatives like the one Ontario is considering. The European Union's *General Data Protection Regulation* (the GDPR),[8] in effect since May 2018, has been a global game-changer, requiring legislative reforms throughout its member states and inspiring reforms beyond. Places as close-by as the UK, Norway, Iceland, and Lichtenstein, and as far away as Japan, Thailand, and Brazil have reformed their data protection laws to align with the GDPR, while others, like India, are in the course of doing so. Gartner predicts that "by 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today".[9] Many of these initiatives are driven by the desire to obtain or maintain "adequacy" status under Article 45 of the GDPR[10] that allows for cross-border data flows and facilitates international trade with the European Union.

The *California Consumer Privacy Act* (the CCPA),[11] another highly influential privacy protection regime introduced in 2018, aims to protect the privacy rights of consumers who are residents of California, backed up by strong enforcement measures. The CCPA is narrower in scope than the GDPR, though in many ways comparable.[12] In the absence of a comprehensive United States federal privacy law, the CCPA has set in motion a wave of similar laws and bills at the state level.[13]

---

[7] Ontario government, "Ontario Delivers Simpler, Faster, Better Services for Ontarians with New Digital Plan" (30 April, 2019) retrieved on August 31, 2020.
[8] Regulation (EU) 2016/679, General Data Protection Regulation.
[9] Gartner, "Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations" (14 September, 2020) retrieved on October 11, 2020.
[10] Article 45, Regulation (EU) 2016/679, General Data Protection Regulation.
[11] 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199].
[12] Future of Privacy Forum "Comparing privacy laws: GDPR v. CCPA" and Practical Law "CCPA and GDPR Comparison Chart" retrieved on August 31, 2020.
[13] See as examples, Maine, *An Act To Protect the Privacy of Online Customer Information,* Nevada Senate Bill No. 220, Massachusetts, *Bill S120 Massachusetts Data Privacy Law,* New York, *Senate Bill S5642 New York Privacy Act,* and Maryland, *Senate Bill 613 Maryland Online Consumer Protection Act*.

Closer to home, Quebec, the first Canadian province to have adopted private sector privacy legislation in 1993, is considering a complete overhaul of its first-generation law. Inspired by the GDPR, the government of Quebec recently tabled Bill 64, "*An Act to modernize legislative provisions as regards the protection of personal information*" (Bill 64).[14] The bill overhauls Quebec's privacy protection regime in both the public and private sectors, with additional individual rights and much stronger enforcement, including the possibility for the Commission d'accès à l'information to institute penal proceedings for offences and impose significant monetary penalties.

Privacy protection has become the "question du jour" that has seized the entire world and Ontario should be commended for reviewing its legislative options amidst this rapidly evolving, increasingly digital, and highly competitive global context.

4. Why Ontario? Why now?

Since 2001, organizations in Ontario that collect, use, or disclose personal information in the course of commercial activity have been regulated by Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[15] While other large Canadian provinces – Quebec,[16] Alberta,[17] and British Columbia[18] – have introduced private sector privacy laws deemed "substantially similar" to PIPEDA, Ontario has not. Accordingly, private sector organizations operating in Quebec, Alberta, and British Columbia are exempted from the application of PIPEDA. In contrast, Ontario-based companies continue to be governed by federal legislation and are subject to the oversight of the federal Office of the Privacy Commissioner (OPC). A legitimate question one might ask is: why should Ontario consider changing its status under PIPEDA now, after twenty years?

One obvious option would be to keep the *status quo* in Ontario. After all, PIPEDA has many virtues, including its purpose statement, which seeks to balance individual privacy rights with the legitimate needs of commercial organizations to collect, use, and disclose personal information. PIPEDA has long been lauded as technology-neutral, principles-based legislation, and flexible in its structure and design. It was among the first privacy regimes in the world to explicitly adopt the principle of accountability. Ontario-based companies have had almost 20 years to adapt their practices to PIPEDA, and PIPEDA enjoys partial adequacy status under the GDPR — *at least for now*.

Despite these virtues, the public record is littered with criticisms by stakeholders on all sides who have grown frustrated with PIPEDA over the years.[19] The refrain often revolves around the commonly held view that PIPEDA has fallen behind the times, is ill suited to the current context, and is no longer fit for its intended purpose. Privacy advocates complain of its weak enforcement mechanisms and lack of teeth. Companies complain of its informed consent requirement that has

---

[14] National Assembly of Quebec, "Bill 64, An Act to modernize legislative provisions as regards the protection of personal information" (12 June, 2020) retrieved on August 1, 2020.
[15] *Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)*.
[16] P-39.1 - *Act Respecting the Protection of Personal Information in the Private Sector* and *Organizations in the Province of Quebec Exemption Order, SOR/2003-374*
[17] *Personal Information Protection Act Chapter P-6.5* and *Organizations in the Province of Alberta Exemption Order, SOR/2004-219*
[18] *Personal Information Protection Act*, S.B.C. 2003, c. 63 and *Organizations in the Province of British Columbia Exemption Order, SOR/2004-220*
[19] House of Commons, "Report of the Standing Committee on Access to Information, Privacy and Ethics", 42nd Parliament, 1st Session (February 2018) retrieved on August 25, 2020.

become unrealistic and unworkable in an era of big data analytics and artificial intelligence. Legal scholars complain of its awkward form and structure that are the by-product of its historical origins[20] and which are inherently difficult to interpret and apply in practice.

Although PIPEDA was destined for a major reform last year, no new privacy bill had been tabled at the time of writing this submission.

Even if PIPEDA undergoes reform, it could still never become what it cannot be. The effectiveness of PIPEDA will always be limited by its constitutional underpinnings. The federal government passed PIPEDA under its authority to regulate trade and commerce under section 91(2) of the *Constitution Act, 1867*[21] (the Constitution) on the basis that personal information was a commodity and its protection was an interprovincial issue.[22] However, to protect PIPEDA from constitutional challenge, the drafters left open the door for a province to adopt a substantially similar law and thereby exempt covered organizations within that province.[23] As noted above, British Columbia, Alberta and Quebec availed themselves of this option by adopting, and/or having declared as substantially similar, private sector privacy legislation based on their provincial authority over property and civil rights under section 92(13) of the Constitution.

As the provinces' authority to regulate property and civil rights is arguably broader than the federal government's authority to regulate trade and commerce, a made-in-Ontario private sector privacy law could extend coverage beyond commercial activities to include the non-commercial activities of unions, charitable organizations, professional associations, or political parties. It could also protect the privacy of employees in provincially-regulated workplaces, protect personal information in the context of litigation, and address important issues such as substitute decision-makers or the minimum age thresholds for valid consent online – all of which are primarily matters of provincial jurisdiction which PIPEDA does not (and cannot) speak to.

Moreover, as public-private partnerships continue to increase, having each collaborating partner subject to oversight by different data protection authorities creates a risk of regulatory redundancy. For example, breach incidents involving a public sector institution and a third-party service provider,[24] or cases involving unauthorized disclosures,[25] have given rise to investigations by both the IPC and the OPC, each having to exercise their respective jurisdiction over related aspects of the same facts and issues. Large-scale public-private projects in Ontario (such as the now-defunct Quayside project involving Sidewalk Labs)[26] potentially have to comply with multiple privacy laws, subject to different regulators, making these types of innovative initiatives more challenging to get off the ground.

---

[20] Canadian Standards Association "CAN/CSA-Q830-96 Model Code for the Protection of Personal Information" (March 1996), retrieved on October 12, 2020.
[21] Constitution Act, 1867 (UK), 30 & 31 Vict, c 3, reprinted in RSC 1985, App II, No 5, s. 91(2).
[22] House of Commons, "Report of the Standing Committee on Access to Information, Privacy and Ethics", 42nd Parliament, 1st Session (February 2018), at page 13, retrieved on August 25, 2020; citing House of Commons, Hansard, 2nd Session, 36th Parliament, Number 9 (22 October, 1999), at page 537.
[23] PIPEDA, section 26(2).
[24] Office of the Information and Privacy Commissioner of Ontario, "Privacy Complaint Report PR16-40" (20 January 2019) retrieved on September 1, 2020.
[25] Office of the Information and Privacy Commissioner of Ontario, "PHIPA Order HO-013" (16 December 2014) retrieved on September 1, 2020.
[26] Sidewalk Labs, "Why we're no longer pursuing the Quayside project — and what's next for Sidewalk Labs" (7 May, 2020), retrieved on October 12, 2020.

From the individual complainant's perspective, this regulatory morass tends to create unnecessary confusion as to which law applies and to which oversight body one should complain. For organizations, this can lead to duplicative investigative processes and potentially conflicting outcomes. From the taxpayers' standpoint, this can be perceived as needless bureaucracy and a waste of valuable resources. For policy-makers, it risks impeding innovation and dissuading global investors, setting back the government's economic objectives.

5. Key principles

One of the virtues of PIPEDA we would recommend be followed in any substantially similar privacy law is its principles-based approach. Inspired initially by the Organization for Economic Cooperation and Development (OECD), a principles-based approach tends to weather technological changes and fare better over time. Even still, PIPEDA's fair information principles annexed as Schedule 1 to the Act are in need of significant recalibration. More than 24 years have passed since the development of the CSA Model Code[27] when smartphones, social media platforms, virtual assistants, and other sensor-laden devices were not even conceived of.

While Purpose Specification, Consent, and Collection Limitation continue to be relevant principles, a more modern private sector privacy law would need to reconsider the weight ascribed to them relative to other principles in certain circumstances. For example, in an era of artificial intelligence and advanced data analytics, organizations must rely on enormous volumes of data, which runs directly counter to collection limitation. Data are obtained, observed, inferred, and/or created from many sources other than the individual, rendering individual consent less practicable than it once was. The very object of these advanced data processes is to discover the unknown, identify patterns and derive insights that cannot be anticipated, let alone described at the outset, making highly detailed purpose specification virtually impossible.

On the other hand, other principles have taken on much greater significance since their original articulation in 1996 and need to be amplified. For example, the Accountability principle has evolved far beyond designating "a person" responsible for privacy compliance, adopting and implementing privacy policies, and providing employee privacy training. Today, chief privacy officers have become critical members of an organization's C-suite, reporting directly to the organization's highest level, with very defined roles and responsibilities.[28] Accountability obligations have evolved into more enhanced data stewardship responsibilities[29] and privacy impact assessments – once a mainstay of a robust privacy management program – have broadened into ethical impact assessments,[30] or algorithmic impact assessments.[31] Most importantly, today's understanding of accountability requires not only that an organization assumes responsibility for compliance but that it stands ready to *demonstrate* compliance to regulators on demand.

---

[27] Canadian Standards Association "CAN/CSA-Q830-96 Model Code for the Protection of Personal Information" (March 1996), retrieved on October 12, 2020.
[28] According to Gartner's Predictions for the Future of Privacy 2020, "(b)y year-end 2022, more than 1 million organizations will have appointed a privacy officer (or data protection officer) … up from only a few thousand official privacy officers worldwide before the GDPR took effect in 2018."
[29] The Information Accountability Foundation, The Essential Elements of Accountability, 2019, retrieved on October 15, 2020.
[30] The Information Accountability Foundation, "Canadian Assessment Framework: Big Data Assessment for Canadian Private Sector Organizations Project" (2017) and "Data Stewardship Accountability, Data Impact Assessments and Oversight Models" (2018), retrieved on October 15, 2020.
[31] Government of Canada, "Algorithmic Impact Assessment" (2020), retrieved on October 12, 2020.

In the case of AI systems that have significant potential to impact people's lives and reputations, accountability requirements are becoming even more exacting. At its most recent meeting, the Global Privacy Assembly passed a unanimous resolution on "Accountability in the Development and Use of Artificial Intelligence" urging those responsible for the development or use of AI systems to implement additional accountability measures. These include, among other things: robust testing prior to deployment and ongoing monitoring to identify and address any potential bias; an assessment of the risks to human rights; intervention by accountable human actors; auditability of AI systems; implementation of whistleblower/reporter mechanisms; and, multi-stakeholder consultations to identify wider socio-economic impacts and ensure "algorithmic vigilance".[32]

Accuracy, a principle not frequently invoked until now,[33] will take on greater importance as automated decision-making increases the risks of drawing unfair or erroneous inferences about people with potentially serious impacts on their lives. Accordingly, the accuracy principle would need to be expanded to incorporate data quality obligations to ensure that data used for automated decision-making are accurate, complete, and up-to-date. A more expansive view of accuracy (to include qualitative notions of relevance and appropriateness) should also be considered to help guide social networking sites and other online platforms faced with increasing numbers and complexity of take-down requests as individuals strive to preserve their reputational integrity.

The Safeguarding principle has come to be better understood and framed in terms of risk mitigation, rather than failsafe methods of protecting privacy. Deidentification, pseudonymization, and other privacy-enhancing technologies, along with robust breach incident response plans, security controls, auditing programs, and threat risk assessments, have become part of the expected arsenal of risk mitigation measures against cyberattacks and other security threats. Moreover, the safeguarding principle has come to include a temporal aspect, with the expectation that many of these privacy and security safeguards must be built into new products or services at their very design stage and be carried out throughout the entire life cycle of the data as part of a robust security governance process.

The Openness or Transparency principle, once a matter of making privacy policies accessible on an organization's website, has evolved into a much more complex principle, including notions of algorithmic transparency and explainability.

The principle of Individual Access and Correction has also recently expanded to encompass individual rights to data mobility or portability, empowering people to switch providers and take their data with them.

Finally, there are essential new principles that are conspicuous in their absence and should be considered and clearly articulated in any modern privacy legislative initiative. These include an overarching principle of Proportionality, which, together with reasonableness, should serve as the lens through which the law's other provisions are interpreted and applied to avoid excessive data processing and ensure a balanced consideration of intended benefits relative to risks. Principles of Lawfulness, Fairness and Equity have become critically important to protect individuals *and*

---

[32] Resolution on "Accountability in the Development and Use of Artificial Intelligence" adopted at the 42nd Closed Session of the Global Privacy Assembly (October 2020).

[33] Accuracy complaints represented 2% of total complaints accepted by the OPC in 2019-2020, up from just 1% last year. Office of the Privacy Commissioner of Canada, "2019-2020 Annual Report to Parliament on the Privacy Act and Personal Information Protection and Electronic Documents Act".

groups from downstream discriminatory impacts of automated data use and profiling. In very high-risk information systems involving artificial intelligence and robotics, serious thought should also be given to the role that the Precautionary principle may play in helping support pre-emptive measures to avoid or minimize risks and potential harms in the face of scientific uncertainty.

6. Ontario's opportunity in a nutshell

For all the reasons above, Ontario should be commended for proactively reflecting upon whether the time has come to introduce its own private sector privacy legislation. Doing so may open up a whole range of new opportunities at this particular juncture, including:

- To broaden the scope of the law's application to bring other organizations into the fold, which continue to operate in a legislative vacuum due to the constitutional limits of PIPEDA;

- To level the playing field with greater certainty and more predictable rules, harmonized with that of other jurisdictions, that incentivize responsible use and respectful treatment of data, while prohibiting unfair and inappropriate data management practices;

- To design a more comprehensive and coherent regime, with a better integrated, streamlined, and agile oversight mechanism to address some of the most complex data challenges that lie at the intersection of public and private sectors;

- To selectively adopt those aspects of other privacy statutes that have proven to work well over time, while replacing the less enviable elements with more effective approaches that are nevertheless harmonized and interoperable with those other laws;

- To modernize and refresh the foundational principles of a modern privacy law that provide the guardrails for responsible data processing and help support sustainable decisions and actions over time; and,

- To create a forward-looking, world-class private sector privacy law capable of rising to the emerging challenges of a digital age in a manner that, ultimately, works best for the people and organizations of Ontario and accords with local values and culture.

We now address each of the eight topics included among the "Key Areas for Reform" in the Discussion Paper.

B. Comments on the government's proposed areas for reform

1. Transparency

Transparency requirements set the rules for what information organizations must disclose about their personal information handling practices. Transparency requirements can serve multiple purposes:

1) They are essential for obtaining meaningful consent to the collection, use, and disclosure of personal information from customers, considering the likely age, language, literacy level, and other characteristics of the intended audience;

2) They afford an essential opportunity for the broader public to understand and compare data management practices across competitors in an industry; and,

3) They allow relevant oversight bodies to scrutinize an organization's practices so regulators can ensure compliance and hold them to account.

Transparency to consumers, the public, and regulators may take different forms. For example, consumers may need succinct notices, with creative pop-ups, visuals, icons, or infographics, to help inform their consent choices in real-time, sometimes on small screens, at the point of decision-making. The public may generally be provided with high level, plain-language information about an organization's data activities on its website, presented in a layered format for those who want to receive more comprehensive information. Regulators may require more detailed, technical information, including confidential commercial information and security-related information, to perform an in-depth review and analysis.

To date, generic privacy policies have been the primary vehicle through which organizations attempt to be transparent. However, in practice, privacy policies are often lengthy and opaque. Highly legalistic statements often have little to do with informing individuals and more to do with protecting organizations from potential liability. As is well known, excessively long policies tend to become noise and can result in information overload that is non-actionable. This is demonstrated by the well-documented tendency of many individuals, even the most sophisticated and discerning consumers, to click past lengthy and overly legalistic privacy policies without actually reading them.[34]

This "transparency deficit in the digital age" has spurred many privacy advocates and industry thought leaders to reframe the debate on data transparency by closing the gap between legal transparency and user-centric transparency.[35] As a result, there are many emerging best practices on how to present information in a way that is understandable to users (based on their needs and viewed from their perspectives), which should be considered and encouraged in setting expected standards.[36]

If Ontario enacts private sector privacy legislation, the transparency requirements it includes will be the critical lynchpin to its success. If thoughtfully designed, a modern approach to transparency can be far more effective than it is today, helping increase consumer and public trust in online products and services, which is key to growing and sustaining the digital economy.

Transparency is an essential component of any private sector privacy framework and should figure as one of its most important principles. That said, we caution against providing overly prescriptive transparency requirements in the law itself. Instead, transparency should be promoted through flexible means such as regulations or guidelines established by the regulator,

---

[34] Obar and Oeldorf-Hirsch, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services" (April 2016), Milne and Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices" (204) and Cranor and McDonald "The Cost of Reading Privacy Policies" (2008), retrieved on October 12, 2020.

[35] The Center for Information Policy Leadership, "Reframing Data Transparency" (30 June, 2016) retrieved on October 12, 2020.

[36] The Center for Information Policy Leadership, "Ten steps to develop a multilayered privacy notice", retrieved on September 7, 2020; "Berlin Privacy Notices Memorandum" at page 15, (2004) and Law Journal Newsletters, "A Notice Does Not Notify Unless It Can Be Understood" (April 2006) retrieved on September 9, 2020.

in consultation with relevant stakeholders. Alternatively, sector-specific codes of practice could be developed by industry from the ground up, subject to regulatory endorsement or approval. Such flexible tools would supplement the law, yet allow Ontario's transparency requirements to evolve and adapt to the specific industry and technological context.

Transparency has also emerged as a critical issue in the context of automated decision making, which may include profiling.[37] Artificial intelligence systems rely on processing large amounts of personal information. When used for decision-making and predicting consumer or individual behaviour, artificial intelligence systems may introduce not only privacy risks, but also other related risks, such as discrimination and bias. Increasingly, these systems are being deployed with limited to no human involvement, yet can have a significant impact on individuals, such as whether they are blacklisted from certain services across an industry, reported to financial regulators or law enforcement, or turned down for employment or a loan.[38]

The GDPR includes transparency rules that require organizations to inform individuals about the existence of automated decision-making, provide "meaningful information" about the logic involved, and describe the "significance and envisaged consequences" of the decision, while also providing the individual the opportunity to contest the decision and obtain human intervention.[39]

Transparency can also be found as a key principle in emerging ethical AI frameworks. Canada's Federal guiding principles for the *Responsible Use of Artificial Intelligence* expect government to be transparent about how and when they use AI and to "provide meaningful explanations about AI decision-making, while offering opportunities to review results and challenge these decisions."[40]

Internationally, the OECD's AI Principles of 2019 (since adopted by the G20) also affirm, "there should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them."[41] Principle 5 (Democratic Participation) of the Montreal Declaration for Responsible Development of Artificial Intelligence[42] states that AI decisions "affecting a person's life, quality of life, or reputation should always be justifiable in a language that is understood by the people who use them or who are subjected to the consequences of their use" and "(t)he code for algorithms, whether public or private, must always be accessible to the relevant public authorities and stakeholders for verification and control purposes."[43] Most recently, the Global Privacy Assembly has adopted a unanimous Resolution urging organizations responsible for the development of use of AI systems to provide clear and

---

[37] According to the UK ICO, "automated individual decision-making does not have to involve profiling, although it often will." The GDPR defines profiling as: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. [Article 4(4)], Information Commissioner's Office, "Rights related to automated decision making including profiling" retrieved on September 7, 2020.

[38] The Conversation, "Did artificial intelligence deny you credit?" (13 March, 2017) retrieved on September 8, 2020.

[39] Articles 13(2)(f) and 22, Regulation (EU) 2016/679, General Data Protection Regulation

[40] Government of Canada, "Responsible Use of Artificial Intelligence." (July 28, 2020) retrieved on September 28, 2020.

[41] The OECD AI Principles (May 2019) retrieved on September 28, 2020.

[42] Montréal Declaration Responsible AI, "Montreal Declaration for a Responsible Development of AI" (2018)

[43] Montréal Declaration Responsible AI, "The Declaration"(2018)

understandable explanation of the use of AI, the logic involved, the data being used and the types of automated decisions being made.[44]

Increased transparency regarding automated or partially automated decisions would help people to better understand how decisions are made about them and help ensure such decisions are fair and reasonable, or challengeable if they are not.

2. Consent

Academics, public interest advocacy groups, privacy regulators, and the public have all lamented the challenges that new technologies and business models pose to PIPEDA's consent-based model of privacy protection.[45] Some claim that individuals can exercise better control over their personal information using meaningful, informed consent as the primary vehicle. Others argue that it is growing increasingly impossible to identify, explain, or even predict every purpose for which personal information may be used or disclosed in the future, making informed consent a fictional concept. What is widely accepted among all camps is that the current consent model in PIPEDA is in critical need of reform.

Were Ontario to adopt its own private sector privacy law, there is a tremendous opportunity to learn from the PIPEDA experience and reframe the role of consent accordingly. On the one hand, if meaningful, consent can work well as the appropriate mechanism for allowing individuals to make their own choices and exercise greater autonomy and control over their personal information. On the other hand, there are situations in which meaningful consent is simply impracticable, unreasonable, or inappropriate. It would need to be supplemented, if not replaced, by more effective protections and accountability controls to minimize risks to individuals and ensure responsible use of personal information in support of economically and socially beneficial innovation.

In Canada, private sector privacy laws are currently structured around consent as the principal gateway for permissible processing unless an exception to consent applies. Should this hierarchy of rules be preserved, the challenge will be to modernize the consent exceptions to account for new digital realities that were not anticipated when these laws were originally adopted. Rather than design for narrow and specific scenarios, such exceptions would have to build in the necessary guardrails *at the level of principle*, so they could accommodate different situations and provide sufficient flexibility to evolve.

Some might propose that the solution lies in a GDPR-like architecture by adopting multiple grounds for lawful processing of data, whereby consent is only one such ground on the same and equal footing as other alternative bases. However, we believe that non-governmental organizations should first be required to consider whether they can obtain meaningful consent and stand ready – if asked – to demonstrate why they *cannot or should not* do so before turning to permissible exceptions for processing. This approach would be more in keeping with Ontario values that promote individual autonomy and respect consumer choice. Whenever it is reasonable, appropriate, and practicable for people to decide for themselves, they should be given the opportunity to do so.

---

[44] Resolution on "Accountability in the Development and Use of Artificial Intelligence" adopted at the 42nd Closed Session of the Global Privacy Assembly (October 2020).
[45] Office of the Privacy Commissioner of Canada, "Submissions received for the consultation on consent"

Informed, voluntary, and capable consent

Where there is direct contact between an individual and an organization involving a relatively straightforward transaction, there will be ample opportunity to obtain consent for the collection, use, and disclosure of personal information. However, to be valid, such consent must be informed and voluntary, and the person providing it must be legally capable of doing so.

Consent will only be informed where it is reasonable to expect that the individual understands the nature, purpose, and consequences of what is being asked. This condition turns critically on the transparency requirements discussed above, tailored as necessary to suit the intended audience. It is also a dynamic, ongoing process that requires updating individuals with new information as it evolves or becomes available to ensure that the individual continues to agree with the purported collection, use, or disclosure of their personal information.

Voluntary consent cannot be obtained through obfuscation or deceptive claims. Individuals must not be unduly pressured or rushed into accepting unfair conditions. They must be given the choice to take on certain risks and either accept or decline any options or features that are not integral to the product or service they are seeking. They must also have the continuing right to revoke their consent at any time or request the deletion of information that is no longer required to deliver a service, subject to applicable legal or contractual restrictions.

Legal capacity to provide consent must likewise be accounted for. A substitute decision-making framework (currently absent from PIPEDA) must be available for those legally incapable of consenting and especially vulnerable to online fraud and abuse.

Young people engaging with each other through social media platforms, using ubiquitous internet-based tools and applications for play, and increasingly engaged in internet-based learning as our educators grapple with the challenges brought on by the pandemic, are in particular need of protection. Other jurisdictions, including the European Union and the United States, have established parental consent requirements for minors under a prescribed age. The *Children's Online Privacy Protection Act* in the United States requires parental consent to collect personal information from children under the age of 13. The GDPR requires parental or guardian consent to access online services for children under the age of 16.[46] Similarly, the Ontario government will need to consider the age at which minors should be able to provide meaningful consent regarding their personal data and establish rules for substitute consent – in line with other consent regimes within provincial jurisdiction.

A consent-based regime must also consider the appropriate form of consent that will be required depending on the circumstances. Express consent should be required where information is sensitive in nature (such as financial, political, racial, religious, genetic, biometric, sex, or health-related personal information). Express consent should likewise be required where a purported collection, use, or disclosure is not within the scope of what an individual would have reasonably expected. For example, where an organization purports to make a new use or disclosure of personal information that is outside the context that the individual initially contemplated when they provided consent to its collection in the first place. Or, where a new organization unknown to the individual (such as a third-party processor) wishes to make independent use of an individual's personal information for their own commercial purposes, unrelated to the service or product the individual expects to receive from the data controller.

[46] However, Member States are permitted to implement general contract laws that set a lower age threshold, provided the age is not below 13 years old.

On the other hand, there will be circumstances where implied consent may be acceptable. For example, where the personal information is not sensitive in nature, where the purported collection, use or disclosure of personal information can be reasonably expected as being within the context originally contemplated and related to the product or service being sought, and where simple, practical and accessible means are provided for individuals to opt-out, if they so choose.

Exceptions to consent

The critical success of a well-balanced private sector privacy law rests on its ability to anticipate and account for a flexible list of consent exceptions that allow organizations to collect, use and disclose personal information without consent.

There are already some well-known and widely accepted consent exceptions in Canadian privacy laws, including:

- where collection, use, or disclosure are permitted or required by law;
- for purposes of responding to a subpoena, warrant, or court order;
- in cases of life or health emergencies, or for humanitarian reasons;
- for purposes of debt collection, investigation, or fraud detection;
- for law enforcement or national security purposes; and
- for employment management purposes.

In the increasingly complex data ecosystem in which we find ourselves, there are some modern business needs and realities for which there is currently no clear consent exception in PIPEDA, and would need to be articulated in a new Ontario law.

For example, a standard business practice of many organizations today is to outsource part of their data processing functions to third-party service providers to gain efficiencies and leverage economies of scale to remain competitive. Consent does not work well in these business-to-business transactions involving what could be multiple data processors, within or outside Canada, that have not been directly engaged by the individual. Many of these outsourced functions involve highly complex technologies and arrangements.[47] It has proven to be significantly challenging, if not impossible, for individuals to understand how their personal information is processed, and keep up with the sheer number of third-party processors, let alone exert any realistic measure of control over organizations' outsourcing decisions.

There is also a growing level of uncertainty around the applicable consent rules for outsourcing under PIPEDA, both from the data custodian and data processers' perspectives. With no explicit consent exception for outsourcing, the prevailing view, according to regulatory guidance, has been that as long as the third party processes personal information on behalf of the data

[47] Automated vehicles are a good example of a technology that involves these complexities. Today's generation of connected and automated vehicles include hardware components, user interface devices, mobile software management, short range mobile device connectivity, audio services, and application providers, often developed and provided by parties other than the automobile manufacturer, many of whom may have access to a wide array of personal information: Rajen Akalu, Ph.D., "A Privacy Code of Practice for the Connected Car" retrieved on September 9, 2020.

custodian, within the scope of the original consent obtained, and subject to clear notification and contractual requirements, no new consent should be required.[48]

That regulatory position was revisited in a number of recent findings[49] that identified certain statutory ambiguities and gave rise to vigorous policy debates around how PIPEDA should be interpreted in its current state, and/or improved as part of a broader reform initiative. These recent debates revealed the need for a much clearer, more predictable statutory regime, laying out the respective roles and responsibilities of data custodians and data processors as part of a robust and coherent accountability framework for third party processing. For example, Chapter 4 of the GDPR sets out explicit legal requirements for data controllers and processors and could be highly instructive for Ontario in this regard.[50]

Another area in which the absence of an explicit consent exception is proving to be increasingly difficult is in the area of data analytics and artificial intelligence systems. Today, virtually all companies are experimenting with data to find new ways to innovate and maintain a competitive advantage. They are increasingly processing data in highly complex ways to, among other things:

- derive new insights about potential consumers and identification of like audiences to improve the effectiveness of advertising or marketing strategies;
- tailor new products and services based on customer profiles;
- refine and enhance risk assessment processes to inform lending or insurance decisions or for fraud detection purposes;
- provide greater convenience, enhance process efficiencies, or facilitate access to products or services, etc.

The risks associated with these highly complex forms of data processing are typically glossed over and captured under the general rubric of "improving our services," buried in lengthy and opaque consent policies and terms of use. Data protection regulators, governments, legislators, privacy advocates, consumer protection groups, and most responsible organizations all recognize with near certainty that such consent, even if obtained, is not "informed" in any meaningful sense. Yet, unchallenged, this so-called consent currently provides legal license for organizations to engage in complex, high-risk practices without further scrutiny, unless a complaint is filed or a breach becomes known.

The hardline alternative, to declare this consent legally invalid and prohibit such processing in the absence of a permissible exception, would bring to a grinding halt many important data initiatives on which our current economy relies. The inadvertent effect might be to snuff out innovation, and forestall – or even prevent – the realization of many important initiatives with serious potential to solve important societal problems and create significant health, social, and economic benefits.

To address this dilemma, many are calling for another consent exception. Defining the contours of a new consent exception, its appropriate threshold, and related conditions for allowing these types of high-performance computing processes is key to ensuring a well-balanced private sector

---

[48] Office of the Privacy Commissioner of Canada, "Guidelines for processing personal data across borders" (2009) retrieved on October 13, 2020.
[49] See Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2019-001" (Equifax) (9 April, 2019) and "PIPEDA Report of Findings #2020-001" (TD Canada Trust) and (4 August, 2020), retrieved on September 30, 2020.
[50] Chapter 4, Regulation (EU) 2016/679, General Data Protection Regulation.

privacy law that is both workable from an operational perspective and sustainable from a public trust perspective.

Trying to foresee all future insights derived from the data and possible uses that may be made of it is virtually impossible. Unknown risks associated with inherent algorithmic bias and potential downstream discriminatory harms are difficult to anticipate, let alone address. Making lending or insurance decisions, running credit checks or security screening, disclosing risky behavior to financial regulators or law enforcement, based on erroneous inferences or biased information, could have devastating economic or reputational effects on peoples' lives. Serving up tailored ads based on an individual's profile may be relatively benign, but tailoring the version of world news a person receives could have serious long-term social impacts by perpetuating existing held views, entrenching our differences and reducing our tolerance for diversity. Training machines to categorize individuals through facial recognition systems can result in grave mistakes and undermine the very dignity of human beings.[51] Using social networking platforms to encourage civic engagement to vote is one thing, but allowing third parties to surreptitiously use online information to influence or nudge a person's voting behavior is viewed to be a serious affront to democracy and crosses the line of what is considered socially acceptable.[52]

To deal with these serious risks, many global thought leaders are calling for a new regulatory framework to provide more meaningful protection for individuals when dealing with particularly complex, high-risk uses of data. Such a framework must include stronger accountability, transparency, and regulatory oversight based on an independent assessment and robust process for balancing relevant ethical principles. An enhanced process must consider risks and benefits, not only for the organization, its employees, and shareholders but more broadly, for individuals affected as well as society as a whole.[53]

Carefully and thoughtfully defining the high-risk circumstances where consent is not reasonable, appropriate or practicable will be key to the success of a made-in-Ontario private sector privacy law. Defining the conditions and enhanced controls that can protect individuals' privacy in alternative ways, will bring greater clarity and predictability to the rules governing the respectful treatment of data, while restoring the integrity of the consent model in situations where it does work. To put it succinctly, this will be the most challenging piece to get right in any new private sector privacy law.

3. Erasure

With the ever-growing capture and generation of information that occurs as people go about their lives, they inevitably leave a lengthy digital trail behind. Much of this digital trail (also referred to as "digital exhaust") will be accessible via the internet, potentially indefinitely, including information that individuals post about themselves, or information posted about them by others. For some,

---

[51] America Civil Liberties Union, "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots" (26 July, 2018), The Guardian, "Google's solution to accidental algorithmic racism: ban gorillas"(12 January, 2018), New York Times, "Wrongfully Accused by an Algorithm" (24 June, 2020), BBC News, "South Wales Police in court over facial recognition system" (24 June, 2020) and C. Garvie, A. Bedoya, and J. Frankle. The perpetual line-up: Unregulated police face recognition in America. Technical report, Georgetown University Law School, Washington, DC, 10 2018.

[52] Canadian Parliamentary Review, "The Inception of an International Grand Committee" Article 2 / 14, Vol 42 No. 3 (Fall), (November 2019), retrieved on October 13, 2020.

[53] The Information Accountability Foundation, "A Path to Trustworthy People Beneficial Data Activities", A Report prepared for Innovation, Science and Economic Development Canada (March 2020), retrieved on October 15, 2020.

this content may include embarrassing, inaccurate, outdated, or irrelevant information. With the ease of online search, this information is widely available to millions on an indeterminate basis, with significant reputational impacts on individuals. For instance, potential employers, lenders, or landlords can make decisions based on an individual's online profile, often without the person's knowledge or control.

The right to erasure (or the right to be forgotten) has emerged in modern data protection laws as a means by which individuals can request that online personal information about them be taken down or de-indexed. These concepts of deletion and/or de-indexing are complex and distinct measures that require careful consideration by the government. The following section focuses specifically on the application of these concepts in the context of information posted online.

Deletion at source

If Ontario proceeds to introduce private sector privacy legislation, people should be provided with the ability to remove information that they themselves provided to an online platform for publication on the internet. This is based on the general principle that consent is revocable and individuals should be able to request the deletion of information that is no longer required to deliver a service, subject to applicable legal or contractual restrictions. In particular, minors deserve special consideration given that they may have little choice but to engage online, and should be granted the freedom of experimentation and self-discovery at a young age without worrying about the permanence of information they post about themselves online.[54]

In certain limited circumstances, an individual should also have the right to request the deletion of personal information about them posted on the internet by someone else. These limited circumstances might include situations where the information was obtained illegally (such as unauthorized collection or covert recording) or posted illegally (such as copyright infringement or in violation of a court order).

However, we would caution against expanding these limited circumstances too broadly. An unqualified right to deletion risks infringing upon the freedom of expression guaranteed under section 2(b) of the *Canadian Charter of Rights and Freedoms* (Charter). Freedom of expression has been given a "large and liberal interpretation" by the Supreme Court of Canada. It has been found to protect not just speakers (or writers), but listeners (or readers) as well. Accordingly, the concept of freedom of expression has been interpreted as incorporating the derivative right of individuals to receive and access information necessary to permit meaningful discussion on a matter of public interest.[55]

Ultimately, the government should strive to arrive at a framework for processing deletion requests in a manner that will ensure an appropriate balance between the right to privacy and other Charter rights, such as freedom of expression, including the derivative right of individuals to access information on matters of public interest. This may include requiring websites and platforms to establish a process for receiving and processing take down requests at first instance, subject to

---

[54] See for example, California's Business and Professions Code, Chapter 22.1 on *Privacy Rights for California Minors in the Digital World* that requires website operators and social media platforms to enable minors to request and obtain deletion of content they post about themselves, Cal Bus. & Prof. § 22581(a)(1); see also, Office of the Privacy Commissioner of Canada, "Draft OPC Position on Online Reputation", (January 2018) retrieved on August 22, 2020.

[55] *Edmonton Journal v. Alberta (Attorney General)*, [1989] 2 SCR 1326, pp. 1339-1340; *R. v. National Post*, [2010] 1 SCR 477 at para. 28.

an independent appeal mechanism for adjudicating disputes between an individual requesting deletion, the organization hosting the information, and, as necessary, the individual who has posted the information.

De-indexing

A right to de-indexing grants individuals the right to request that certain online content linked to their name be removed from the results returned by a search engine. When information is de-indexed, the source material continues to be available on the internet, but the information will not be discoverable through a name-based query. Essentially, the information remains online but becomes more difficult for others to find. De-indexing is somewhat less controversial than a broad right of deletion due to its more limited interference with the right to freedom of expression.

If passed, Quebec's Bill 64 would grant individuals the right to have any hyperlink attached to their name de-indexed where dissemination contravenes the law or a court order.[56] It would also grant individuals the right to have a hyperlink attached to their name de-indexed where dissemination causes serious injury to reputation or privacy that outweighs the public's right to be informed and freedom of expression (and the request does not exceed what is necessary for preventing the injury).[57]

Quebec's Bill 64 sets out several criteria for this assessment:

- whether the person concerned is a public figure;
- whether the person concerned is a minor;
- whether the information is up to date and accurate;
- the sensitivity of the information;
- the context in which the information is disseminated;
- the time elapsed between the dissemination of the information and the de-indexing request; and,
- where the information concerns a criminal or penal procedure, the obtaining of a pardon, or the application of a restriction on the accessibility of records of the court of justice.

In our view, the assessment framework set out in Quebec's Bill 64 provides an interesting model for Ontario to examine were it to consider undertaking something similar.

In principle, the IPC supports granting individuals a right to request that their personal information be de-indexed where the information is inaccurate, inappropriate, outdated, or no longer relevant. Such requests must be examined on a case-by-case basis, taking into consideration countervailing interests of freedom of expression and access to information in the public interest. In line with our comments on deletion, the government should explore a framework that recognizes and balances these rights and interests relative to one another. This should include a defined process and/or body for managing de-indexing requests that is regarded by all impacted parties as being independent, legitimate, and workable.

[56] Section 28.1, National Assembly of Quebec, "Bill 64, An Act to modernize legislative provisions as regards the protection of personal information" (12 June, 2020) retrieved on August 1, 2020.
[57] Section 28.1, National Assembly of Quebec, "Bill 64, An Act to modernize legislative provisions as regards the protection of personal information" (12 June, 2020) retrieved on August 1, 2020.

The question remains, though, who is best placed to receive takedown requests and carry out such an assessment? Some believe that it is inappropriate to rely on search engines to make such fundamental decisions about the balance between the right of privacy and freedom of expression. In the Report of the Standing Committee on Access to Information, Privacy and Ethics, "*Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*," the ETHI Committee suggested that one way of addressing these concerns would be to adopt a solid legislative framework and have an objective third party with the proper expertise to implement it, such as a tribunal.[58]

More realistically, however, the government could consider enshrining in Ontario a similar mechanism to that which is currently in place in the EU and seems to work relatively well.[59] This mechanism would impose on search engines the obligation to complete an initial review and decision on de-indexing requests. It would also require search engines to provide individuals with the right to seek further redress through an independent oversight body, like the IPC, should they disagree with the search engine's decision.

4. Portability

Data portability is an explicit right for individuals to receive their personal information in a standardized digital format and move their information to another organization. As noted in the government's Discussion Paper, data portability is important for both user control and competition. According to the Competition Bureau:

> Barriers to switching, called switching costs, can lead to less competitive markets where incumbents "lock-in" their customers and new competitors have no way to grow their business. The potential benefits of increased data portability for competition and productivity could be profound.[60]

A right to data portability has been established in many jurisdictions, including in the European Union,[61] and California,[62] and under a sectoral-based approach in Australia[63] (granting a right for individuals to access specified data in the banking and energy sectors). It is also included in the recently proposed amendments to Quebec's Bill 64.[64] Ontario can learn from the implementation experience and models created in other jurisdictions, and the ongoing consideration of this issue by Canadian governments. When the European Union enacted the GDPR, one survey[65] ranked the data portability requirements as the most difficult compliance obligation. To address these

---

[58] House of Commons, "Report of the Standing Committee on Access to Information, Privacy and Ethics", 42nd Parliament, 1st Session (February 2018) retrieved on August 25, 2020.
[59] See, for instance, Google's Transparency Report on Requests to Delist under EU Privacy Law: https://transparencyreport.google.com/eu-privacy/overview
[60] Competition Bureau, "Submission to the Government of Ontario on Ontario's Data Strategy" (29 November, 2019) retrieved on August 27, 2020.
[61] Article 20, Regulation (EU) 2016/679, General Data Protection Regulation.
[62] Section 1798 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199].
[63] A "Consumer Data Right" was created by amending the *Competition and Consumer Act 2010*, *Australian Information Commissioner Act 2010* and *Privacy Act 1988, Treasury Laws Amendment (Consumer Data Right) Bill 2019,* and Australian Government, "Consumer Data Right" (June 2020) retrieved on September 1, 2020.
[64] Section 27, National Assembly of Quebec, "Bill 64, An Act to modernize legislative provisions as regards the protection of personal information" (12 June, 2020) retrieved on August 1, 2020.
[65] International Association of Privacy Professionals, "IAPP-EY Annual Privacy Governance Report 2017" retrieved on September 7, 2020.

concerns, the IPC supports the province's inclusion of a right to data portability in a private sector privacy framework, subject to the following important considerations.

Interoperability

The GDPR grants individuals the right to receive their own personal data in a "structured, commonly used and machine-readable format." The European Data Protection Board (EDPB)[66] issued guidance to support implementation of the GDPR standard, which states:

> The terms "structured," "commonly used," and "machine-readable" are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. In that way, "structured, commonly used, and machine readable" are specifications for the means, whereas interoperability is the desired outcome.[67]

The GDPR does not impose specific recommendations on the format of the personal data to be provided given the wide range of potential data types. The EDPB has indicated that the most appropriate format will differ across sectors.[68]

The Ontario government should recognize that organizations may require support to operationalize this requirement. As noted by ISED, there may be a need to develop common approaches to data transfer, reception, and use, potentially through sector-specific codes of practice or the development of technical industry standards.[69] The goal of ensuring common approaches could also be reached by the enactment of sector-specific industry regulations developed in consultation with relevant stakeholders of that sector.

Scope

The government also should carefully consider the scope of any data portability requirements and the potential need to enact reasonable exceptions. For instance, the GDPR provides for exceptions where compliance would reveal a trade secret or would not be technically feasible.

There remains some uncertainty regarding the scope of the portability requirements established in Article 20 of the GDPR. One report suggested that the portability requirements were being interpreted too broadly by regulators.[70] The report was based on guidance issued by the EDPB, where the Board clarified that the right to data portability covers data provided knowingly and actively by the data subject, and the personal data generated by his or her activity, which can include observed data by organizations. In the same guidelines, however, the EDPB advised that

---

[66] The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). European Data Protection Board, "About EDPB" retrieved on September 7, 2020.

[67] European Data Protection Board, "Guidelines on the right to "data portability" (27 October, 2017) retrieved on August 31, 2020.

[68] European Data Protection Board, "Guidelines on the right to "data portability"" (27 October, 2017) retrieved on August 31, 2020.

[69] Innovation, Science and Economic Development Canada, "Strengthening Privacy for the Digital Age" (21 May, 2019) retrieved on July 30, 2020.

[70] International Association of Privacy Professionals, "European Commission, experts uneasy over WP29 data portability interpretation" (25 April, 2017) retrieved on September 8, 2020.

the scope should exclude “inferred data” and “derived data”, which include personal data that are created by a service provider (for example, algorithmic results).

Like the Ontario government, ISED has posed questions about the scope of portability requirements in its white paper *Strengthening Privacy for the Digital Age: Proposals to modernize the Personal Information Protection and Electronic Documents Act* (“Strengthening Privacy for the Digital Age”), asking for feedback from stakeholders on whether the portability provisions should capture derived data.[71] It would be important to compare feedback received, particularly from organizations that have had to comply with the GDPR, to shed as much practical light on this issue as possible.

5. Oversight, compliance, and enforcement

Modern privacy regimes need to focus on both effective mechanisms to support compliance and enhanced enforcement powers to address serious or egregious non-compliance.

As ISED noted in *Strengthening Privacy for the Digital Age*, a data protection regulator can be most effective when supported by a framework that grants it authority in four key areas:

1. education and outreach
2. proactive advice and dialogue
3. complaints and investigations
4. enforcement tools to address non-compliance.[72]

We strongly agree that the government should explore the full spectrum of regulatory compliance tools.

Compliance support

Amidst increasing calls to help guide and educate organizations and enhance digital literacy among the broader public, a made-in-Ontario private sector privacy law should provide the IPC with a broad and explicit mandate to conduct research, provide education, and issue guidance and advisory opinions. The IPC has a strong and long-standing practice of providing such services to public sector organizations, and the health, child and family services sectors. Subject to sufficient resources and capacity, such services could likewise be extended to private sector organizations that would become subject to a new Ontario law.

Any modern legislative initiative must consider providing the regulator with the ability to deploy some of the agile and cutting-edge regulatory tools that are being widely tested in other jurisdictions. For example, the United Kingdom Information Commissioner’s Office (ICO) offers a wide range of innovative regulatory solutions, and has recently begun beta testing regulatory sandboxes.[73] A sandbox is a safe space where organizations can experiment and test innovative

[71] European Data Protection Board, “Guidelines on the right to "data portability"” (27 October, 2017) retrieved on August 31, 2020.
[72] Innovation, Science and Economic Development Canada, “Strengthening Privacy for the Digital Age” (21 May, 2019) retrieved on August 12, 2020; citing Centre for Information and Policy Leadership, “Regulating for Results: Strategies and Priorities for Leadership and Engagement” (25 September, 2017).
[73] Information Commissioner’s Office, “Sandbox beta phase Discussion Paper ” (March 2019) retrieved on August 20, 2020.

products and services in consultation with the regulator to ensure compliance with legislation.[74] According to the ICO, its sandbox trial has helped organizations deliver new products and services to assure that they have built-in privacy. The ICO further noted that sandboxes have helped their office better understand how organizations are innovating in the use of personal information and where additional ICO guidance may be helpful.[75]

We also encourage the exploration of codes of practice and certification schemes as another proactive compliance tool. There may be many benefits associated with a framework that incentivizes organizations to develop codes of practice proactively, provided there is a role for the oversight body to approve or sanction them. The GDPR encourages the development of codes, particularly for specific sectors and small and medium businesses,[76] and ISED's *Strengthening Privacy for the Digital Age* also explores ways to further incentivize codes, including validation from the OPC.[77]

Complaints and investigations

Increasingly, privacy complaints and investigations cross jurisdictional boundaries. Thus, it will be important to grant authority for the regulator to share information with other data protection authorities, given the need to harmonize investigative processes across provincial and international borders wherever possible. Also, privacy matters can overlap with other regulatory mandates, such as consumer protection agencies or human rights tribunals. Information sharing with other regulators would support cooperation and help ensure that regulatory oversight and responses are streamlined, rather than duplicative or unduly onerous for organizations who experience a data breach across several jurisdictions or undertake a data initiative that raises more than privacy implications.

Processing complaints is an important aspect of a privacy regulator's mandate. However, handling high volumes of complaints can be resource intensive and is not always the most effective or efficient way of protecting Ontarians' privacy from the most serious of risks.[78]

We recommend that any new private sector privacy law should grant the regulator with discretion to determine whether it will investigate complaints received. For example, under the *Personal Health Information Protection Act, 2004*, (PHIPA), the IPC may decide not to conduct a formal review of a complaint for any reason the IPC considers proper, including if the subject of the complaint has adequately responded to it or if another procedure is more appropriate for dealing with the complaint, such as through a health regulatory college. Several other laws provide privacy regulators the authority to decline to investigate complaints that are frivolous, vexatious, made in bad faith, or are an abuse of a right.[79] Additionally, the privacy regulator should have discretion, subject to basic statutory or common law rules of procedural fairness, to determine its own

[74] Centre for Information and Policy Leadership, "Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice" (8 March, 2019) retrieved on August 19, 2020.
[75] United Kingdom Information Commissioner's Office, "Information Commissioner's Annual Report and Financial Statements 2019-20" (20 July, 2020), retrieved on August 21, 2020.
[76] Article 40, Regulation (EU) 2016/679, General Data Protection Regulation.
[77] Innovation, Science and Economic Development Canada, "Strengthening Privacy for the Digital Age" (21 May, 2019) retrieved on August 12, 2020
[78] Centre for Information and Policy Leadership, "Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice" (8 March, 2019) retrieved on August 19, 2020.
[79] For example see, paragraph 12.2(1)(b) of the *Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)*, section 37 of the *Personal Information Protection Act Chapter P-6.5* and section 52 of P-39.1 - *Act Respecting the Protection of Personal Information in the Private Sector*.

investigative and tribunal processes, such as where an expedited or abridged investigation process may be more appropriate.[80]

Enforcement powers

As noted in the Ontario government's Discussion Paper, strong oversight and enforcement powers are crucial to modernizing privacy protections and building public trust and confidence in the data-driven economy. Enforcement mechanisms create incentives for compliance and ensure serious incidents of non-compliance can be effectively addressed. In particular, the IPC supports a proposal to explore a proportionate approach to enforcement based on the size and revenue of an organization and the circumstances of the complaint.

If it proceeds with made-in-Ontario private sector privacy legislation, the government should consider equipping the regulator with enforcement tools such as order-making powers, the ability to administer administrative monetary penalties, the authority to issue production orders, and the ability to perform audits. In the most egregious cases, there should also be a regime for significant offences and fines to be administered by the Attorney General on the regulator's recommendation. Unconscionable data practices, failure to notify in the event of a data breach, knowingly or recklessly contravening the law, obstructing a regulator's investigation, defying a regulator's order, or retaliating against a whistleblower are examples of the types of offences that should figure into a private sector privacy law.

Recent amendments to PHIPA have provided the IPC with the power to order administrative monetary penalties. Internationally, both the GDPR and CCPA provide for monetary penalties for non-compliance, and in the European Union, administrative fines can be imposed by the privacy authority.[81] Recently, Quebec Bill 64 proposes administrative monetary penalties and a regime for fines.

Order making powers are critically important for effective oversight and compliance. The IPC's ability to issue orders significantly enhances our ability to enforce PHIPA and Part X of the *Child, Youth and Family Services Act*. As a last resort, order-making powers encourage organizations to follow guidance and meaningfully participate in alternative dispute resolution processes. Our experience with order-making powers in the public sector has shown that when there is a risk that the IPC will issue an order compelling enforcement, stakeholders are more inclined to reach a mediated solution, which means reduced enforcement and compliance costs for everyone involved, and often results in a more satisfying, robust and quicker resolution of the issues.

The Discussion Paper briefly mentions mandatory breach reporting, a critical and indispensable piece of any modern privacy law. A breach-reporting regime brings greater transparency to data security-related incidents. Many jurisdictions require organizations to notify affected individuals and the privacy regulator once a certain risk threshold is established and imposes sanctions in the event of non-compliance. In line with other provincial and federal privacy statutes and international precedents, the government should require mandatory breach reporting in the private sector, as it does in the health and child and family services sectors. It should also carefully consider the appropriate threshold for reporting to match that in PIPEDA and Alberta's *Personal*

[80] Centre for Information and Policy Leadership, "Regulating for Results: Strategies and Priorities for Leadership and Engagement" (25 September, 2017) retrieved on August 12, 2020.
[81] Article 83, Regulation (EU) 2016/679, General Data Protection Regulation.

Information Protection Act (PIPA)[82] and impose serious consequences for failure to do so. Another important feature of a breach-reporting regime, such as Ontario's PHIPA, requires organizations to keep records of breaches they experience and produce relevant statistics to the regulator on an annual basis.[83] This record-keeping process provides a window into potential trends over time or systemic security risks that require additional attention.

6. De-identification

De-identification is widely recognized as a potential solution for striking an effective balance between privacy protection and innovative data uses. It is a process for removing direct and indirect personal identifiers from a dataset or otherwise transforming the data to help ensure that the individuals in the dataset are not identifiable. According to Ontario's FIPPA, de-identification "means to remove the following information:

1. Information that identifies an individual.
2. Information that could be used, either alone or with other information, to identify an individual based on what is reasonably foreseeable in the circumstances."[84]

What is "reasonably foreseeable in the circumstances" will depend on the state of the data itself and the context in which it is used and/or released. As outlined in the IPC's de-identification guidance, the extent of de-identification required to protect the privacy of individuals, while preserving as much utility in the information as possible, must be assessed as a function of the re-identification risks involved.[85] Accordingly, the government should consider introducing a risk-based assessment framework that requires the consideration of contextual factors, such as:

- the purpose for which the de-identified dataset will be used (a specific, restricted and known purpose v. an unspecified, unrestricted and unknown purpose)
- by whom (an accredited researcher affiliated with a reputable institution, a trusted third party with whom there is a longstanding contractual relationship or an unknown member of the public)
- the user's likely motivations (to derive insights for scholarly or commercial purposes, a motivated intruder or a malicious attacker)
- the environment in which data are intended to be released (release to a trusted agent v. release via a highly controlled data centre v. release via a restricted online portal or open release to the public via the Internet)
- other publicly available datasets (census data, birth and death data, family trees and genealogical websites).[86]

---

[82] Specifically, a "real risk of significant harm." See Alberta *Personal Information Protection Act* s.34.1(1); and the Federal *Personal Information Protection and Electronic Documents Act* s.10.1(1).

[83] Section 6.4 of Ontario Regulation 329/04 made pursuant to the *Personal Health Information Protection Act, 2004*.

[84] Section 49.1(2) of the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31. A similar definition can be found in *Personal Health Information Protection Act, 2004*, S.O. 2004, C. 3 section 2

[85] Office of the Information and Privacy Commissioner of Ontario, "De-identification Guidelines for Structured Data" (June 2016) retrieved on September 1, 2020.

[86] For an overview of different use cases that highlight these various contextual factors, see the Canadian Anonymization Network (CANON)'s Data Sharing Use Cases, retrieved on October 15, 2020.

Re-identification risks also depend on the governance controls in place to protect the data from possibly being re-identified either deliberately or inadvertently. Such controls may include:

- information security safeguards;
- technical, organizational or structural means of segregating datasets;
- due diligence verifications of third parties to whom data will be released;
- user access controls;
- contractual restrictions on any further uses or disclosures;
- confidentiality obligations of users;
- regular compliance monitoring and testing through audits, access logs, re-identification attacks and other risk assessments;
- an effective containment and notification requirement in the event of inadvertent re-identification.[87]

Moreover, to further guard against deliberate re-identification, there should be a clear statutory prohibition against wilfully using or attempting to use information that has been de-identified for the purpose of re-identifying an individual, as was recently introduced in PHIPA.[88]

Recognizing the difficulty of interpreting and applying thresholds in abstraction of context, the relatively low risks of using or disclosing data that have been properly de-identified and the tremendous value that can be derived therefrom, the government may wish to consider exempting de-identified data from consent. By implication, this would bring de-identified data within the scope of the law and require organizations to respect other obligations, such as accountability, security, and transparency, so they are better positioned to manage dynamic risks and ensure the data remain de-identified. Quebec's Bill 64, for example, includes an exception to consent for the use of personal information if the information is de-identified, and is necessary for study or research or statistics.[89] If the Ontario government follows suit by creating an exception to consent for using or disclosing de-identified information for certain purposes, it must be clear that the process of de-identification to get the data in that state should not require consent. Otherwise, the consent exception would become self-defeating.

The GDPR also recognizes partial measures such as pseudonymization, where personal information is coded in such a manner that cannot be attributed to a specific individual without the use of additional information which exists (such as a code key), but is kept separately and protected by technical and organizational measures. The GDPR builds in incentives for organizations to pseudonymize data as a means of helping controllers and processors meet their obligations related to data minimization, security safeguards, and data protection by design. Pseudonymization also allows the internal analyses of data within the same controller when appropriate technical and organizational measures have been taken to ensure that those processing the data are kept separate from those who hold the key. A similar provision would help address the ongoing uncertainty under many Canadian privacy laws as to whether coded information in the hands of the same organization that also holds the code key, can ever be truly de-identified within the meaning of our current statutory definitions.

---

[87] The applicability of these controls will depend on the use case in question, see CANON Data Sharing Use Cases, *ibid*.
[88] PHIPA, section 11.2 and section 72(1)(b.1).
[89] Section 12, National Assembly of Quebec, "Bill 64, An Act to modernize legislative provisions as regards the protection of personal information" (12 June, 2020) retrieved on October 15, 2020.

In any future Ontario private sector privacy law, we would encourage government to define de-identification in a manner consistent with how it is defined under PHIPA and FIPPA to support cross-sectoral data sharing. To further support an interoperable framework beyond Ontario, the government should explore the definitions of de-identification in other jurisdictions and where appropriate, ensure consistency. Under a technology-neutral framework, the government should also ensure that any definitions adopted are not limited to any particular privacy-enhancing technology, given the likelihood that these will evolve and become superseded by others.

We would also recommend that the government consider defining other related terms across the full spectrum of identifiability, including pseudonymization. The goal should be to incentivize organizations to pseudonymize personal data as a way of enhancing protections for individuals, while helping organizations meet their security obligations and facilitate internal data use and analyses provided effective governance controls are in place to separate the code key.

7. Scope and application

The IPC endorses the government's proposal to extend the application of the law to non-commercial organizations. As noted above, the effectiveness of PIPEDA is limited by the federal heads of power. A made-in-Ontario private sector privacy law could address current gaps in PIPEDA*'s* scope of application*,* including employee information held by provincially regulated workplaces and the non-commercial activities of organizations such as non-profits, unions and political parties.

Employees

In Quebec, Alberta, and British Columbia, all employees' personal information is protected by their applicable private sector privacy law. In Ontario, only employees in federally regulated workplaces, such as banks, telecommunication companies, and airlines, are protected under PIPEDA. The privacy of Ontarians working in any other private sector organization remains unprotected.

Yet, as we know, employers across all sectors can hold highly sensitive personal information about their employees, ranging from health information and performance assessments, to personal communications on work-issued devices. The COVID-19 pandemic has only emphasized the vulnerability of employee personal information. For example, media reports suggest that employers are increasingly exploring the adoption of surveillance measures in light of the recent influx of employees working from home.[90] Additionally, employers are engaging in contact tracing and disease monitoring of employees as organizations reopen.[91] Individuals should have the ability to perform their jobs with the confidence that their employer will keep them safe, while also respecting their privacy rights. Accordingly, we recommend that any private sector privacy law in Ontario should apply to all employee personal information to fill this glaring gap in privacy protection.

[90] CBC, "No slacking allowed: companies keep careful eye on work-from-home productivity during COVID-19" (14 May, 2020) retrieved on August 31, 2020.
[91] Professor Teresa Scassa, "Privacy and Contact Tracing: Comments to INDU Committee of the House of Commons" (1 June, 2020) retrieved on July 27, 2020.

Non-commercial organizations

A growing number of organizations, including charitable foundations, associations, unions, professional bodies, etc., are engaging in non-commercial data collection activities, which are not covered under PIPEDA. As the government noted in its Discussion Paper, with which we agree, any future Ontario private sector privacy law must aim to protect personal information regardless of whether it is held by a commercial business or by a not-for-profit organization.

Political parties

We also recommend that the scope of application extend coverage to include political parties. In Ontario, political parties are not covered by privacy laws at either the provincial or federal level. In British Columbia, political parties are subject to the province's private sector privacy legislation, and Quebec's Bill 64 proposes amendments that would establish privacy protections for electors concerning personal information held by political parties.[92]

The large amount of personal information held by political parties, coupled with advances in the technology enabling them to collect, integrate, and analyze data in ways that could not have been previously imagined, reveals a widening gap in protection and oversight of individual privacy rights. This problem is compounded by the fact that increasingly our engagement with political parties is through online platforms. The most effective way of making Ontario's political parties accountable for protecting privacy is by making them subject to Ontario's privacy laws. The public's expectation regarding the right to privacy is the same whether they engage with a private company, the government, or a political party. Citizen trust depends on the measures in place to protect personal information. The Cambridge Analytica revelations shook the public's confidence by shining a light on the ability of third parties to create and sell psychological profiles obtained through analysis of Facebook data for political purposes.[93]

As Professor Teresa Scassa noted, public concern about political parties is mounting: "[t]here have been reports and studies, op-eds and editorials, privacy commissioner complaints, a competition bureau complaint, and even legal action. There is a growing gulf between what Canadians expect when it comes to the treatment of their personal data and the obligations of political parties."[94] We also believe the government should take action to address this issue.

8. Data sharing

We appreciate that there is a need for increased data sharing between organizations, potentially in different sectors, and agree that solutions such as data trusts are worth exploring.

As there is no universal definition of a data trust, the government must consider the intended purpose or role for data trusts, determine which model of data trust is most appropriate for the

[92] National Assembly of Quebec, "Bill 64, An Act to modernize legislative provisions as regards the protection of personal information" (June 12, 2020) proposed amendments to Section 551.1.1 and 551.1.2 of the *Elections Act*, retrieved on August 1, 2020.
[93] Vian Bakir, "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting." (September 3, 2020), retrieved October 12, 2020. See also: Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, PIPEDA Report of Findings #2019-002 (April 25, 2019).
[94] Professor Teresa Scassa "Data Protection Laws and Political Parties: No Half Measures" (16 August, 2020) retrieved on August 27, 2020.

Ontario context and define the conditions under which it can be used. The UK-based Open Data Institute (ODI) has researched data trusts, identifying several types, ranging from a formal legal structure, to less formal repositories of data, and public oversight of data access.[95] ODI has also noted that data trusts can fulfill a range of purposes, such as data sharing and ensuring the safe and secure storage of data, and can take different legal forms, such as a contractual framework (for example, a data sharing agreement), or a public organization that sets and enforces standards.[96]

While data trusts are a relatively recent term of art, there are existing examples of trusted data entities for the government to draw from when determining how to approach this issue. For example, the Institute for Clinical Evaluative Sciences (ICES) is an Ontario-based, independent non-profit organization that allows researchers to access data in a manner that ensures the ongoing privacy and security of the data. ICES must comply with enhanced requirements in privacy legislation, including PHIPA, that go over and above those required of other organizations. Every three years, the IPC must conduct a review of ICES' practices and procedures for protecting the privacy and confidentiality of the personal information and personal health information it receives in order to preserve its status and authorities as a prescribed entity.

As demonstrated by this and other national and international data trust initiatives, both the public and private sectors are turning to different models of data trusts for a range of purposes. When determining whether to facilitate data trusts through made-in-Ontario private sector privacy legislation, we recommend that government consult broadly with various sectors, and privacy and technology experts. Rather than ascribe to a single model, we recommend that the government explore different forms and models of data trusts and consider setting out, either in law or by way of more flexible regulation, the minimum criteria for establishing the trust's authority, composition, mandate, and evaluation criteria. Also, as per our Office's previous public comments on this issue,[97] we recommend that they be subject to regulatory oversight by the IPC as a backstop to ensure true independence and accountability to the people of Ontario.

Supplementary comments on trans-border data flows

An important issue that was not raised in the Discussion Paper, but needs to be addressed, is the regulation of the cross-border transfer of data. Many existing frameworks include requirements to ensure that an appropriate level of privacy and security protection remains in place when data flows across borders.

In Canada, the approach taken to date has held organizations accountable for personal information transferred to other jurisdictions by providing a comparable level of protection through contractual or other means.[98] Regulatory guidelines have been issued regarding the elements to be included in notice requirements to inform individuals of the related risks, though (as noted above) these have been the subject of much recent discussion and controversy in Canada and

[95] The Open Data Institute, "What is a Data Trust?" (8 July, 2018) retrieved on July 31, 2020.
[96] The Open Data Institute, "Data trusts: legal and governance considerations" (April 2019) retrieved on July 27, 2020.
[97] Information and Privacy Commissioner of Ontario, "Open Letter from Commissioner re: Sidewalk Labs' Proposal" (26 September, 2019), retrieved on September 28, 2020.
[98] PIPEDA Principle 4.1.3: "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."

can certainly stand to benefit from greater clarity, predictability and certainty in law.[99] This "accountability" approach provides organizations with the greatest level of flexibility, but remains vulnerable to the laws of the other jurisdiction that may override any contractual arrangements and permit access to data for law enforcement or national security purposes. The challenge will be in finding the appropriate balance that recognizes the pragmatic reality of global trade, while also acknowledging the heightened privacy risks inherent in some legal regimes, relative to others.

The GDPR[100] and its predecessor, Directive 95-46-EC,[101] provide several grounds for enabling cross border data transfers to non-EU countries, including model contractual clauses, binding corporate rules and "adequacy rulings." The latter approach was the means selected in Quebec's Bill 64,[102] though not without criticism.[103] For the same reasons raised by others, we would guard against taking on an overly bureaucratic and laborious exercise of creating an exclusive "allow list" of jurisdictions to which Ontario businesses may be permitted to transfer personal data.

C. Conclusion

In closing, we wish to reiterate our support for a made-in-Ontario private sector privacy law. As demonstrated by the wave of legislative change occurring both domestically and abroad, Ontario's turn has come. The time is now for Ontario to fill the inevitable gaps in coverage that a federal privacy regime will inevitably leave behind, and to design a seamless and well-integrated privacy regulatory framework across its private, public and health sectors. Only by earning Ontarians' trust that their personal data will be treated responsibly, *and respectfully*, will the Ontario government be able to advance its goal of facilitating data-driven innovations for the benefit of all its citizens.

We look forward to learning more about the outcome of the government's consultation process and contributing further to the next stages of this important discussion. While the journey should be an open, inclusive, thoughtful and deliberative one, the final destination must be a modern, balanced and robust privacy regime that both protects individuals' personal data and enables organizations' business needs.

---

[99] See Office of the Privacy Commissioner of Canada, "Guidelines for processing personal data across borders." (January 2009), retrieved October 12, 2020; Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2019-001" (9 April, 2019) and "PIPEDA Report of Findings #2020-001" (4 August, 2020), both retrieved on September 30, 2020.

[100] Regulation (EU) 2016/679, General Data Protection Regulation

[101] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[102] Section 17, Bill 64, An Act to modernize legislative provisions as regards the protection of personal information" (12 June, 2020) retrieved on August 1, 2020.

[103] Jennifer Stoddart, "Quebec takes the lead in privacy law but overreaches." (July 15, 2020), retrieved on October 12, 2020.