



PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC

SUBMISSION OF THE PUBLIC INTEREST ADVOCACY CENTRE ("PIAC")

TO:

Ontario Consultations to Strengthen Privacy Protections of Personal Data

A General Private Sector Privacy Statute for Ontario: A Step in The Right Direction?

16 October 2020

TABLE OF CONTENTS

INTRODUCTION 5

OVERVIEW OF POSITION: PIAC SUPPORTS BOLSTERING PRIVACY PROTECTIONS IN ONTARIO’S PRIVATE SECTOR, BY STRENGTHENING FEDERAL PIPEDA & INTRODUCING PROVINCIAL EMPLOYMENT PRIVACY LEGISLATION..... 5

PIAC & THE CONSUMER INTEREST IN PRIVACY..... 6

PART 1: SUMMARY OF ONTARIO PRIVACY CONSULTATION 6

CONSULTATION ISSUES & PRELIMINARY POSITION OF ONTARIO GOVERNMENT: NEW PROVINCIAL GENERAL PRIVATE SECTOR PRIVACY LEGISLATION WITH BROAD SCOPE, STRONG OVERSIGHT & NEW/ENHANCED RULES 7

PART 2: CONTEXT MATTERS – COMPREHENSIVE CANADIAN PRIVACY LAW REFORM IS URGENTLY NEEDED, DRIVEN BY DIGITAL TECHNOLOGY & GDPR (NEW GLOBAL STANDARD FOR PRIVACY PROTECTION), BUT WOEFULLY STALLED & FRAGMENTAL..... 8

CONTEXT #1: CANADIAN PRIVACY LAW IS EXTRAORDINARILY COMPLEX 8

“Privacy” Means Privacy of “Personal Information”, Broadly Defined 8

Legal Framework For Protecting Personal Information (“Privacy Law”) Governs Its Collection, Use & Disclosure 9

Privacy Law Is Quasi-Constitutional & Recognizes Need To Balance Other Interests 9

Privacy Law Has Myriad Sources & Competent Authorities 10

Canadian Privacy Statutes & Commissioners: A Federal & Provincial/Territorial (“FPT”) Patchwork..... 10

Canadian Privacy Statutes & Commissioners (Overall)..... 10

Canadian Private Sector Privacy Statutes 12

Canadian Privacy Statutes Are Not Rights-Based 13

Canadian Privacy Statutes Have Similarities & Differences 14

Personal Information Is Subject To Multiple, Complex, Overlapping & Inconsistent Canadian Privacy Statutes & When More Than One Applies You Must Comply With All 14

Heart Of Privacy Law Is Privacy Principles & Individual Rights (“Privacy Protections”) 15

Privacy Principles 16

Individual Rights 17

CONTEXT #2: CANADIAN PRIVACY LAW REFORM IS URGENTLY NEEDED, TO BRIDGE DIGITAL PRIVACY GAP & ENSURE MAINTAINED EU “ADEQUACY” STATUS PURSUANT TO GDPR 18

Canadian Privacy Law Reform Is Urgently Needed, To Bridge The Digital Privacy Gap 18

Canadian Privacy Law Reform Is Driven By GDPR, The New Global Standard For Privacy Protection 20

GDPR Overview: Application, Oversight, “Adequacy” Decision/Assessment & Key Features..... 20

GDPR Is New Global Standard For Privacy Protection 21

Canadian Privacy Legislation Not Aligned With GDPR & Spectre of “Adequacy” Challenge Looms Large 22

PIPEDA v. GDPR: Key Differences (“Adequacy Gaps”) 23

Scope/Application 23

Privacy Protections..... 24

Organization Obligations 24

Individual Rights..... 29

Compliance (With Privacy Protections) & Enforcement (Of Non-Compliance)..... 31

Compliance 31

Enforcement 32

CONTEXT #3: CANADIAN PRIVACY LAW REFORM (FPT) IS UNDERWAY BUT WOEFULLY STALLED & FRAGMENTAL 34

Canadian Privacy Law Reform (FPT) is Underway, Showing The Question Is How, Not Whether, To Modernize Privacy Statutes..... 34

Canadian Privacy Law Reform, Especially Federal, Is Woefully Stalled & Fragmental 36

PART 3: PIAC’S POSITION ON CANADIAN PRIVACY LAW REFORM (OVERALL) UNDERPINS OUR RECOMMENDATION IN THIS CONSULTATION – TAKE TWO TRACK APPROACH, WITH IMMEDIATE FOCUS ON “GDPR-IZING” FEDERAL PRIVACY STATUTES & PT STATUTES IN AREAS OF PRIMARILY/EXCLUSIVELY PT JURISDICTION & LONG-TERM AIM OF UNIFIED FEDERAL PUBLIC/PRIVATE SECTOR LEGISLATION 36

FUNDAMENTAL QUESTION THAT BEGS ASKING: IS NEW PT GENERAL PRIVATE SECTOR PRIVACY LEGISLATION (OVERALL) A STEP IN RIGHT DIRECTION?	36
PIAC'S ANSWER: NEW PT GENERAL PRIVATE SECTOR PRIVACY LEGISLATION IS A STEP IN WRONG DIRECTION	37
<i>New PT General Private Sector Privacy Legislation Would Further Fragment Existing Patchwork, Thus Undermining Privacy Protection For Canadians</i>	37
<i>Canadian Privacy Law Reform (Overall) Should Take Two Track Approach</i>	38
TRACK #1: Immediate Focus On "GDPR-izing" Federal Privacy Statutes & PT Statutes In Areas Of Primary/Exclusive PT Jurisdiction.....	38
TRACK #2: Journey Toward Eventual, Necessary & Inevitable Unified Federal Public/Private Sector Legislation.....	39
PART 4: PIAC'S RECOMMENDATION IN THIS CONSULTATION – BOLSTER PRIVACY PROTECTIONS IN ONTARIO'S PRIVATE SECTOR, BY "GDPR-IZING" PIPEDA & INTRODUCING ONTARIO EMPLOYMENT PRIVACY LEGISLATION..	40
RECOMMENDATION #1: BOLSTER PRIVACY PROTECTIONS IN ONTARIO'S PRIVATE SECTOR	40
RECOMMENDATION #2: DO NOT INTRODUCE ONTARIO GENERAL PRIVATE SECTOR PRIVACY STATUTE; INSTEAD, "GDPR-IZE" PIPEDA & INTRODUCE ONTARIO EMPLOYMENT SECTOR PRIVACY LEGISLATION.....	42
<i>Do Not Introduce Ontario General Private Sector Privacy Legislation</i>	42
REASON #1: New Ontario General Private Sector Privacy Legislation Is Inconsistent With PIAC's Position On Canadian Privacy Law Reform	42
REASON #2: New Ontario General Private Sector Privacy Legislation Would Be Ill-Suited For Increasingly Inter-Jurisdictional Personal Information Flows	43
REASON #3: New Ontario General Private Sector Privacy Legislation Would Cause More Problems Than It Solves	43
<i>"GDPR-ize" PIPEDA</i>	43
REASON #1: "GDPR-izing" PIPEDA Is Consistent With PIAC's Position On Canadian Privacy Law Reform	43
REASON #2: "GDPR-izing" PIPEDA is Supported by Key Privacy Stakeholders	44
REASON #3: Jurisdictional Challenges of "GDPR-izing" PIPEDA Are Real But Surmountable	45
<i>Introduce Ontario Employment Sector Privacy Legislation</i>	45
REASON #1: New Ontario Employment Privacy Legislation Is Consistent With PIAC's Position On Canadian Privacy Law Reform.....	45
REASON #2: Workplace Privacy Is Increasingly Contentious, Highlighted By COVID-19 Pandemic	46
RECOMMENDATION #3: "GDPR-IZE" GENERAL PRIVATE SECTOR PRIVACY LEGISLATION (PIPEDA OR NEW ONTARIO STATUTE) BY ENHANCING ITS SCOPE, PRIVACY PROTECTIONS, & COMPLIANCE/ENFORCEMENT ("PIAC-RECOMMENDED PRIVACY RULES")	47
<i>Scope/Application: Expand (Within Constitutional Limits)</i>	47
Preamble & Purpose Statement: Introduce, To Ensure Proper Balance Between Individuals' Right To Privacy & Organizations' "Legitimate Interests"	47
"Personal Information": Clarify & Expand.....	48
Non-Commercial Organizations & Activities: Include (Within Constitutional Limits).....	49
Extraterritoriality: Clarify	49
Periodic Reviews: Maintain	50
<i>Privacy Protections (Overall): Clarify & Enhance</i>	50
Substance: Clarify, Cast In Legal Language & Contemplate Private-Public Partnerships	50
Scalability: Consider Introducing, For Non-Commercial Organizations Only (Especially NFPs & Charities)	51
<i>Organization Obligations: Enhance</i>	51
Privacy By Design ("PbD"): Introduce	52
Transparency: Increase.....	52
Consent: Enhance & Minimize Exceptions/Alternative Bases	53
Consent: Enhance.....	54
Exceptions/Alternative Bases To Consent: Minimize Number & Permit Only Where Consent Not "Reasonably Practicable" & For Narrow Range Of "Prescribed Purposes"	55
"Standard Business Practices": Do Not Introduce Exception	57
De-Identified & Derived Data: Introduce Restrictions & Permitted Uses	57
Data Trusts: Do Not Legislatively Enable Now (Premature).....	60
Necessity & Proportionality: Introduce.....	66
Accountability: Enhance	66
Data Breach, Transfer (To Third Parties/Other Countries) & Localisation: Enhance & Introduce.....	66
Data Breach: Enhance	66

Data Transfers To Third Parties (“Outsourcing”): Enhance	67
Data Transfers To Other Countries: Enhance	67
Data Localization: Introduce, Subject to International Trade Agreement Restrictions.....	68
<i>Individual Rights: Increase & Enhance</i>	<i>68</i>
Rights-based Approach: Introduce.....	68
Right To Be Informed: Introduce.....	69
Right To Access: Enhance	69
Right To Rectification: Enhance.....	69
Right to Restrict & Object To Processing (Overall): Introduce	70
Right To Object To Marketing: Enhance.....	70
Right To Withdraw Consent: Enhance.....	70
Right To Be Forgotten/Erasure: Introduce	71
Right To Data Portability: Introduce.....	72
Right to Request Source of Information: Introduce.....	73
Rights Related To Automated Decision-Making & Surveillance: Introduce	73
Children’s Rights (Overall): Introduce	75
<i>Oversight, Compliance & Enforcement: Strengthen</i>	<i>76</i>
Compliance Tools: Enhance.....	77
“Demonstrable” Accountability: Introduce	77
Privacy Impact Assessment (“PIA”): Enhance	78
Record-Keeping: Introduce	78
Data Protection Officer (“DPO”): Enhance.....	79
Self-Regulation Mechanisms: Encourage, But Not As Replacement For Legislated Obligations & Strengthened	
Enforcement Tools	79
Research Capacity: Enhance	79
Enforcement Tools: Enhance.....	80
Binding Rule-Making: Introduce	80
Investigation & Audit: Enhance.....	81
Financial Penalties: Enhance	82
Fines (Imposed By Courts): Extend & Increase.....	82
Administrative Monetary Penalties (“AMPs”) (Imposed by Privacy Commissioners): Introduce – See Below	83
Binding Orders & AMPs: Introduce.....	83
Private Right of Action & Statutory Damages: Enhance	84
Scalable Enforcement: Introduce, For Mitigating/Aggravating Factors	85
CONCLUSION: SUMMARY OF PIAC RECOMMENDATIONS.....	86
APPENDIX: BIBLIOGRAPHY	87
GOVERNMENT SOURCES (CANADIAN).....	87
OTHER SOURCES (CANADIAN & INTERNATIONAL).....	90

INTRODUCTION

OVERVIEW OF POSITION: PIAC SUPPORTS BOLSTERING PRIVACY PROTECTIONS IN ONTARIO'S PRIVATE SECTOR, BY STRENGTHENING FEDERAL PIPEDA & INTRODUCING PROVINCIAL EMPLOYMENT PRIVACY LEGISLATION

1. The Public Interest Advocacy Centre (“PIAC”) is pleased to provide the Government of Ontario (“Ontario government”) with our submission to its “Consultations to Strengthen Privacy Protections” launched on August 13, 2020¹ (“Ontario Privacy Consultation”). According to the Ontario government, this consultation responds to “continually heard” concerns about the province’s privacy protections that have “been further highlighted during the COVID-19 outbreak, which has resulted in Ontarians relying more on digital platforms to carry out day-to-day tasks”.²
2. PIAC is intervening on behalf of Canadian, especially Ontarian, consumer-citizens. PIAC supports strengthening privacy protections in Ontario’s private sector, by strengthening the federal *Personal Information Protection and Electronic Documents Act*³ (“PIPEDA”) and introducing provincial employment privacy legislation. In this submission, “employment privacy” is used synonymous with “workplace privacy”.
3. This PIAC submission has four parts:
 - **Part 1:** Summarizes the Ontario Privacy Consultation.
 - **Part 2:** For context, describes the urgent need for comprehensive Canadian privacy law reform. This includes a high level overview of current Canadian private sector privacy legislation.
 - **Part 3:** Provides an overview of PIAC’s position on Canadian privacy law reform (overall), which grounds our recommendations in this consultation.
 - **Part 4:** Recommends **bolstering privacy protections in Ontario’s private sector by “GDPR-izing” PIPEDA and introducing Ontario employment privacy legislation**. However, focuses on **GDPR-izing general private sector privacy legislation – PIPEDA or a new Ontario statute – by enhancing its scope, privacy protections (both organization obligations and individual rights), and compliance/enforcement**.
4. We believe our submission offers a consumer-centric and unique perspective on the important issues the Ontario government must address in deciding on the outcomes of the Ontario Privacy Consultation. In particular, we believe that our recommendations: are realistic; would improve the alignment and interoperability of Canadian privacy legislation with other jurisdictions, especially key trading partners such as the European Union (“EU”), pursuant to the *General Data Protection Regulation*⁴ (“GDPR”); recognize and properly balance individuals’ human right to privacy with private organizations’ (especially businesses’) “legitimate interests” (especially commercial) in collecting, using, and disclosing personal information; and, thereby, enhance public trust in privacy, businesses, and digital technology, which is vital to maximize public participation in the digital economy and preserve our democracy.

***Note: short-form citations correspond to long-form citations in Appendix: Bibliography**

¹ Ontario consultation news release.

² Ontario consultation news release.

³ S.C. 2000, c. 5. When referring to PIPEDA, we mean Part 1 of PIPEDA, which addresses privacy (i.e., sets out rules for personal information handling in the course of a commercial activity) and not Parts 2-5, which deal with other issues (i.e., related to electronic documents).

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - OJ L 119, 4.5.2016, p. 1–88.

PIAC & THE CONSUMER INTEREST IN PRIVACY

5. **PIAC.** PIAC is a national not-for-profit organization and registered charity that represents the interests of consumers, and in particular, vulnerable consumers in important public services.⁵ PIAC has been actively engaged in privacy issues since the early 1990s, with representatives sitting on the Canadian Standards Council Committee that led to the introduction of PIPEDA, filing complaints with the Office of the Privacy Commissioner of Canada (“OPC”, “OPCC”, “Canadian Privacy Commissioner”, or “Privacy Commissioner of Canada”) on privacy standards in consumer transactions throughout the early 2000s, and publishing several reports on PIPEDA and consumers. We have also filed Part 1 Applications with the Canadian Radio-television and Telecommunications Commission (“CRTC”) regarding the role of telecommunications service providers (“TSPs”) in digital technologies and privacy, most recently in September 2020, on the subject of digital contact tracing technology (“DCTT”).
6. **“Consumer” interest.** The term “consumer” has evolved and continues to evolve alongside changes in the communications system and broader communications environment. As CRTC recently stated: “The Internet and digital technology have transformed social, economic, cultural and civic participation by Canadians, making way for a new type of citizen – one who is engaged as a creator, consumer and a full participant in the digital society and economy”.⁶ Breaking down barriers and systemic issues that prevent or limit meaningful participation by Canadians – as consumers and citizens – in the digital economy remains a fundamental mandate of PIAC. For this reason, all references to “consumers” in this intervention should be read as references to “citizen-consumers”. PIAC acknowledges that “much academic ink has been spilt over whether there is a genuine distinction between citizens and consumers, who are after all the same people”⁷, so suffice it here to state PIAC’s belief that citizen-consumers have *integrated* interests rather than an oft-attributed “*duality of interests*”⁸.
7. PIAC’s perspective on the Ontario Privacy Consultation and its impact on the privacy interests of Ontarians as consumers is provided next.

PART 1: SUMMARY OF ONTARIO PRIVACY CONSULTATION

8. On August 13, 2020, the Ontario Ministry of Government and Consumer Services launched the Ontario Privacy Consultation, originally open until October 1, 2020, but subsequently delayed to October 16, 2020.
9. Details on the consultation are provided in the following Ontario government documents (“Ontario government consultation documents”):
 - “News Release: Ontario Launches Consultations to Strengthen Privacy Protections of Personal Data”, Ontario Government, August 13, 2020, online: <https://news.ontario.ca/en/release/57985/ontario-launches-consultations-to-strengthen-privacy-protections-of-personal-data> (“Ontario consultation news release”);
 - “Consultation: Strengthening Privacy Protections in Ontario”, Ontario Ministry of Government and Consumer Services, August, 13, 2020 (last modified September 22, 2020), online: <https://www.ontario.ca/page/consultation-strengthening-privacy-protections-ontario> (“Ontario consultation website”);
 - “Public Consultation - Reforming Privacy in Ontario's Private Sector”, Ontario’s Regulatory Registry, online: <https://www.ontariocanada.com/registry/view.do?language=en&postingId=33967> (“Ontario’s Regulatory Registry”); and

⁵ Online: <https://www.piac.ca/>

⁶ CRTC BTLR submission, p. 13.

⁷ To inform, educate and entertain? British broadcasting in the twenty-first century, p. 11.

⁸ See e.g., Ofcom review of public service television broadcasting – Phase 1 – is television special?, p. 2 (“Ofcom’s core mission is to further the interests of the citizen-consumer... duality of interests”).

- “Ontario Private Sector Privacy Reform: Improving Private Sector Privacy for Ontarians in a Digital Age – Discussion Paper”, Ontario Government, August 13, 2020, online: <https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45105> (“Ontario consultation paper”).

CONSULTATION ISSUES & PRELIMINARY POSITION OF ONTARIO GOVERNMENT: NEW PROVINCIAL GENERAL PRIVATE SECTOR PRIVACY LEGISLATION WITH BROAD SCOPE, STRONG OVERSIGHT & NEW/ENHANCED RULES

10. According to the Ontario government consultation documents, the province aims to “improve our province’s privacy protection laws”, specifically “to create a legislative framework for privacy in the province’s private sector” (“**proposed Ontario legislation**”).
11. With this aim, the Ontario government “seek[s] advice on ways to”⁹:
 - **Transparency**: Increase **transparency**, providing individuals with more detail about how their information is being used by private organizations (businesses and non-businesses).¹⁰
 - **Consent**: Enhance **consent** provisions by “allowing individuals to revoke consent at any time”, and adopt “an ‘opt-in’ model for secondary uses of their information”.¹¹
 - **Right to erasure/be forgotten**: Introduce a right for individuals to request information related to them be **deleted or de-indexed**, subject to limitations.¹²
 - **Right to data portability**: Introduce a right for individuals to obtain their data in a standard and **portable** digital format, giving them greater freedom to change service providers without losing their data.¹³
 - **De-identified & derived data**: Introduce requirements for (i.e., restrictions on), and opportunities to use (i.e., permitted uses for), data that has been **de-identified and derived** from personal information, to clarify applicability of privacy protections.¹⁴
 - **Data trusts**: Create a legislative framework to enable the establishment of **data trusts** “for privacy protective data sharing”.¹⁵ Data trust is defined as “a legal mechanism that enables an organization’s data to be governed by a trusted third party, to ensure the transparent and accountable use of that data. They operate under legal agreements that follow existing intellectual property and privacy protection laws. Currently, no jurisdiction in Canada has a legislative framework for data trusts”.¹⁶
 - **Scope & application**: Expand the **scope and application** of the legislative framework to include “non-commercial organizations, including not-for-profits, charities, trade unions and political parties”.¹⁷
 - **Oversight, compliance & enforcement**: Increase **oversight, compliance, and enforcement** powers for the Ontario Information and Privacy Commissioner (“Ontario Privacy Commissioner” or “IPC”), to ensure businesses comply with the law, including the ability to impose penalties.¹⁸

(“proposed Ontario rules”)
12. The Ontario government consultation documents state that these “key areas for reform” are “not an exhaustive list” and “reflect new areas of consideration for Ontario based on legal requirements introduced in other jurisdictions”, particularly GDPR, implemented by the European Commission on May 25, 2018, which “significantly strengthened privacy protections in the European Union by introducing more robust

⁹ Ontario consultation new release, p. 3; Ontario consultation website.

¹⁰ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3; Ontario consultation website.

¹¹ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3; Ontario consultation website.

¹² Ontario consultation news release, p. 3; Ontario consultation paper, p. 3; Ontario consultation website.

¹³ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3; Ontario consultation website.

¹⁴ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3; Ontario consultation website.

¹⁵ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3; Ontario consultation website.

¹⁶ Ontario consultation news release, p. 3.

¹⁷ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3; Ontario consultation website.

¹⁸ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

requirements for consent, transparency and enforcement, and provided individuals with greater control over their personal data”.¹⁹

13. The context of the Ontario privacy consultation matters. For this reason, it is discussed next, followed by PIAC’s response to the proposed Ontario legislation and rules. Since our response is partly based on, and flows from, our overall position on Canadian privacy law reform, this too is outlined. For clarity, in this submission, PIAC uses “private organizations” (aka “private sector organizations” or “organizations”) as an umbrella term and specifies “commercial organizations” (aka “businesses”) and “non-commercial organizations” (aka “non-businesses”) where meant.²⁰ Private organizations are distinguished from “public organizations” (aka “public sector organizations” or “government institutions”). “Privacy rules” is an umbrella term for legislative rules that govern the collection, use, and disclosure of personal information, including privacy protections (i.e., organization obligations and individual rights), which are specified where meant.

PART 2: CONTEXT MATTERS – COMPREHENSIVE CANADIAN PRIVACY LAW REFORM IS URGENTLY NEEDED, DRIVEN BY DIGITAL TECHNOLOGY & GDPR (NEW GLOBAL STANDARD FOR PRIVACY PROTECTION), BUT WOEFULLY STALLED & FRAGMENTAL

14. Comprehensive Canadian privacy law reform – defined as reform of *private and public* sector privacy legislation (“legislative privacy framework”) – is urgently needed, driven by digital technology and GDPR, the new global standard for privacy protection. Law reform is underway, but it is woefully stalled and fragmental. Before discussing reform of Canadian privacy law, it is important to understand its current state.

CONTEXT #1: CANADIAN PRIVACY LAW IS EXTRAORDINARILY COMPLEX

15. Understanding the current state of Canadian privacy law is difficult, because it is extraordinarily complex.

“PRIVACY” MEANS PRIVACY OF “PERSONAL INFORMATION”, BROADLY DEFINED

16. **Privacy.** “Classically understood as the right to be left alone, the concept of privacy in today’s high-tech world has taken on many new dimensions.”²¹ For this reason, there are many typologies of privacy²², including privacy of *personal information and communication (unmediated and mediated)* – often referred to as “informational privacy”²³ – which is the primary focus of privacy protection laws in Canada²⁴.
17. **Personal information.** “Personal information”, including in digital format (“personal data”), is defined very broadly under Canadian privacy statutes (see details below) as “information about an identifiable individual”²⁵ (e.g., PIPEDA, subs. 2[1] and *Privacy Act*²⁶ s. 3).²⁷ PIAC has long argued that this expansive definition should not be confused with the much narrower and privacy-limiting concept of “personally identifiable information (PII)” which is an American concept that has no place in Canadian law. According to Osler, Hoskin & Harcourt LLP: “Generally, information will be deemed to be about an ‘identifiable individual’ where it is *reasonably possible* for an individual to be identified through the use of that information, alone

¹⁹ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

²⁰ PIAC’s terminology differs from the Ontario government, which often uses “organizations” to mean non-businesses. See e.g., Ontario consultation website (referring to “businesses and organizations”) and Ontario consultation paper, p. 1 (referring to “private businesses and organizations”). Non-businesses include not-for-profits (“NFPs”), charities, trade unions, professional associations, and political parties.

²¹ Canada’s Federal Privacy Laws: Background Paper, p.1.

²² See e.g., A Typology Of Privacy (identifying “eight plus one primary types of privacy”).

²³ See e.g., Supreme Court Of Canada Decision Raises Interesting Issues About Jurisdiction Over Privacy-Impactful Technologies.

²⁴ See e.g., Canada’s Federal Privacy Laws: Background Paper, p. 1.

²⁵ See e.g., Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 54.

²⁶ R.S.C., 1985, c. P-21 (“Privacy Act”).

²⁷ Current definitions of personal information in FPT privacy statutes: public sector – Federal s. 3; BC Sch. 1; AB s. 1(n); SK s. 24(1); MB Defns; ON s. 2(1); QC s. 54; NS s. 3; PEI s. 1; NB s. 1; N&L s. 2; YK s. 3; NWT N/A; Nun s. 2; and private sector – Federal s. 2(1), AB s. 1(1)(k), BC s. 1; QC s. 2.

or in combination with other available information”²⁸ (“reasonable possibility test”). However, it is increasingly hard to know whether information held by entity X could be used to identify an individual when combined with information held by entity Y or available on the Internet, meaning that “more information may qualify for protection as ‘personal information,’ even though it does not directly identify an individual on its own”.²⁹ For this reason, the historical distinction between “personal data” and “population-level, anonymous data” is increasingly blurry (a point revisited in Part 2).

18. **Types of personal information.** Types of personal information include: telephone number (landline and cell), home address, email address and messages, Internet protocol (“IP”) address; birth date, age, height, weight, blood type, DNA code, fingerprints, voiceprint, health status (e.g., COVID-19 positivity); race/colour, national/ethnic origin, religion, marital status; medical, criminal, and employment records; income, financial transactions (purchases, spending habits, banking information, credit/debit card data, loan/credit reports), tax returns; social insurance number (“SIN”), driver’s licence, other identification numbers; activities (online and offline); personal opinions; photos and contact lists; location data (because it can reveal user activity patterns); and metadata.³⁰ Canadian law has taken an expansive approach to interpreting certain personal information available on mobile devices and the Internet (e.g., mobile apps, IP addresses, and online behavioural advertising).³¹ Some categories of personal information are regarded as “sensitive”.

LEGAL FRAMEWORK FOR PROTECTING PERSONAL INFORMATION (“PRIVACY LAW”) GOVERNS ITS COLLECTION, USE & DISCLOSURE

19. The Canadian legal framework for protecting personal information (“privacy law” or “data protection law”³²) fundamentally protects personal information by governing its *collection, use, and disclosure* (“*sharing*”). Sensitive personal information, such as health information, generally has more stringent protections. For example, “personal health information” (“PHI”), which is defined in PIPEDA in a very detailed but expansive manner³³, is always regarded as “sensitive” under PIPEDA and therefore attracts requirements of explicit consent to any collection, use, or disclosure (see details below).

PRIVACY LAW IS QUASI-CONSTITUTIONAL & RECOGNIZES NEED TO BALANCE OTHER INTERESTS

20. **Quasi-constitutional.** “The right to privacy is an internationally recognized right”.³⁴ However, Canada does not have an explicit right to privacy, meaning the word “privacy” does not appear in its constitution, specifically in the *Canadian Charter of Rights and Freedoms*³⁵ (“Charter”).³⁶ Instead, Canada has: “construed a general right to privacy from other rights in (its) constitutional catalog (...) connected most strongly to the protection against unreasonable search and seizure or the right to make certain fundamental choices without the interference of government, but also (...) anchor(ed) in other constitutional rights (...)”³⁷ (e.g., right to freedom of belief and expression, right against self-incrimination, and right to life, liberty, and

²⁸ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 54 (emphasis added). See also: *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, para. 34.

²⁹ Expectations: OPC’s Guide to the Privacy Impact Assessment Process, March 2020.

³⁰ Brookings Report, *Bridging the Gaps: A Path Forward to Federal Privacy Legislation*, p. 32 (re: “precise” location data, online activities, metadata, noting these are included in certain US statutory definitions of “sensitive data”); Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps (re: photos, contact lists, “location information”); Expectations: OPC’s Guide to the Privacy Impact Assessment Process (re: personal opinions); and OPC a Guide for Individuals Protecting your Privacy (re: other listed items).

³¹ See e.g., Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps; The Privacy, Data Protection And Cybersecurity Law Review - Edition 6: Canada (citing PIPEDA Case Summary #2009-010 – Report of Findings: Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection and Office of the Privacy Commissioner of Canada, 'Policy Position on Online Behavioural Advertising', 6 June 2012, https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/bg_ba_1206/).

³² See e.g., *Modernizing Canada’s Privacy Act*.

³³ PIPEDA, subs. 2(1).

³⁴ A Data Privacy Day Conversation With Canada’s Privacy Commissioner.

³⁵ PIPEDA, subs. 2(1).

³⁶ Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), c 11.

³⁷ *Modernizing Canada’s Privacy Act*.

³⁸ A Typology of Privacy, pp. 511-512 (brackets added).

security of the person³⁸). Consequently, Canadian privacy law is accurately described as “quasi-constitutional”.³⁹ The quasi-constitutional status of Canadian privacy law contrasts with the explicitly rights-based approach to privacy taken by other jurisdictions with heightened legal privacy protections, such as the EU pursuant to GDPR.

21. **Recognizes need to balance other interests.** Canadian privacy law “(has) always recognized the need for balancing of interests. Privacy, as a moral or legal principle, does not trump all other laws or interests”⁴⁰, including public health and safety. PIAC’s view on finding the *proper* balance between privacy and public health-safety in the specific context of DCTT related to COVID-19 and future pandemics is detailed in our recent position paper entitled “A ‘Privacy First’ Canadian Public Policy Approach to Digital Contact Tracing (“DCTT”) Related to COVID-19 & Future Pandemics”⁴¹ (“PIAC Position Paper on DCTT and Privacy”).

PRIVACY LAW HAS MYRIAD SOURCES & COMPETENT AUTHORITIES

22. Canadian privacy law has myriad sources – a mix of statutes, regulations, and common law (i.e., decisions by judges, tribunals, and labour arbitrators) – and competent authorities, including: privacy statutes and privacy commissioners; sector-specific statutes with privacy provisions and their respective regulators (e.g., *Telecommunications Act*⁴² and CRTIC); and privacy torts, other protections, and courts. The rest of this submission focuses on privacy statutes and privacy commissioners that oversee compliance with the privacy legislation in their respective jurisdictions.

CANADIAN PRIVACY STATUTES & COMMISSIONERS: A FEDERAL & PROVINCIAL/TERRITORIAL (“FPT”) PATCHWORK

23. The “paramount issue for privacy legislation” is “setting boundaries for how covered entities can collect, use, and share personal information”.⁴³

CANADIAN PRIVACY STATUTES & COMMISSIONERS (OVERALL)

24. **Canadian privacy statutes.** There are Canadian statutes *specifically aimed at protecting personal information*, at the federal and PT (including municipal) level⁴⁴ (“Canadian privacy statutes” or “Canadian privacy legislation”), governing personal information that is held by:

Comprehensive Privacy Statutes (FPT)

- *Public sector organizations* (aka “government institutions” or “public bodies”) (“public sector privacy legislation”)
- *Private sector organizations engaged in commercial activities* (aka “businesses”) (“private sector privacy legislation of general application” or “general/dedicated private sector privacy legislation”)

Private Sector/Industry-Specific Privacy Statutes (PT Only)

- *Health sector organizations*⁴⁵, in context of providing healthcare services (“health sector privacy legislation”, “health privacy legislation” or “healthcare privacy legislation”)

³⁸ A Typology of Privacy, p. 153 and fn 93; OPC a guide for individuals protecting your privacy.

³⁹ OPC a Guide for Individuals Protecting Your Privacy (noting “[t]he Supreme Court of Canada has stated that the Privacy Act has ‘quasi-constitutional status’, and that the values and rights set out in the Act are closely linked to those set out in the Constitution as being necessary to a free and democratic society.”)

⁴⁰ COVID-19 and Privacy: Artificial Intelligence and Contact Tracing in Combatting The Pandemic (bracket added).

⁴¹ PIAC Position Paper on DCTT and Privacy.

⁴² S.C. 1993, c. 38, online: <https://laws.justice.gc.ca/eng/acts/T-3.4/> (“Telecommunications Act” or “Telecom Act”).

⁴³ Brookings Report, Bridging the Gaps: a Path Forward to Federal Privacy Legislation, p. 27.

⁴⁴ Some PTs have privacy legislation that applies to municipalities: Modernizing Canada’s Privacy Act.

⁴⁵ Public as well as private.

- *Employers* in context of the employer-employee relationship (“employment sector privacy legislation”, “employment privacy legislation”, or “workplace privacy legislation”)

25. The Canadian Bar Association (“CBA”) emphasizes the “complex privacy framework in Canada has almost forty privacy statutes covering the public and private sectors”.⁴⁶ A high-level summary of FPT privacy legislation and its application to personal information (“PI”) is provided in the following Table (see details below), which reveals that what statute(s) applies depends on the nature and level of the entity involved and the type of personal information:

Covered Entity (Type/Level)	Protected Information (Type)	Federal Statute	PT Statute
Government (federal/PT – incl. employers)	PI (incl. employee and PHI)	Privacy Act (federal government)	Public sector privacy act (PT government) (all PTs have legislation)
Business (federal/PT)	PI (can incl. employee and/or PHI [statute-specific])	PIPEDA (federal or *PT business) * <u>unless</u> GiC Exemption Order re: <i>intra-PT data flow</i> (see next column)	Private sector privacy act of general application (PT business – intra-PT data flow) (AB, BC, QC have legislation “substantially similar” to PIPEDA)
Health sector organization (federal/PT – government or business)	PHI only	Privacy Act (federal government) PIPEDA (federal or *PT business) * <u>unless</u> GiC Exemption Order re: <i>intra-PT data flow</i> (see next column)	Health sector privacy act (PT government or business – intra-PT data flow) (ON, NB, NFLD + LD, NS have legislation “substantially similar” to PIPEDA)
Employer (federal/PT – government or business)	Employee PI only	Privacy Act (federal government) PIPEDA (federally-regulated business)	Public sector privacy act (PT government) Employment sector privacy act (<i>provincially-regulated</i> business) (AB, BC, and QC have legislation)

26. **Canadian privacy commissioners.** Canadian privacy statutes are administered by independent privacy and/or access to information commissioners (“privacy commissioners” or “privacy regulators”) in each jurisdiction, each heading an organization or office (“privacy office”), including the Privacy Commissioner of Canada and OPCC at the federal level and, in Ontario, the Ontario Privacy Commissioner and Office of the Information and Privacy Commissioner of Ontario (“IPC”). In this submission, references to officials and their offices are used interchangeably.

27. Privacy commissioners report to their respective legislatures and, in addition to overseeing the relevant privacy statutes, have the power to issue regulatory guidance (“guidance”), which is not legally binding, to help entities subject to privacy statutes understand their privacy-related obligations. Privacy commissioners have exercised this power – individually and collectively – to issue guidance on privacy and myriad specific sectors and activities, including digital technologies. Most privacy commissioners have the power to investigate and decide upon complaints from the public, albeit their findings may or may not be “enforceable”, depending on the legislation.

⁴⁶ CBA’s Response to ISED’s Proposals to Modernize PIPEDA.

CANADIAN PRIVATE SECTOR PRIVACY STATUTES

28. Canadian *private sector* privacy statutes are the focus of this submission and therefore warrant further attention.
29. **Federal *general private sector* privacy statute.** PIPEDA applies to personal information collected, used, and disclosed by:
- federal works, undertakings, and businesses (“FWUBs” or “federally-regulated employers”); and
 - private “organizations” in the course of “commercial activities”⁴⁷ that are international, inter-PT, and within a PT that does not have “substantially similar” legislation (see details below).
- Commercial organizations (businesses) by definition engage in commercial activities and therefore are covered. Non-businesses do not typically engage in commercial activities and therefore are not covered *unless and to the extent* they are engaged in commercial activities (a determination that “will vary depending on the facts of each case”⁴⁸) unless the non-business is a type expressly excluded/exempted or treated as exempt from the act (e.g., political parties⁴⁹). The commercial activity connection for non-businesses is consistent with constitutional limits placed on federal legislation (i.e., the Government of Canada’s [“GoC”] reliance on its constitutional jurisdiction over general trade and commerce to enact PIPEDA).⁵⁰
30. PIPEDA does not apply to the personal information of employees (“employee personal information” or “personal employee information”), except for the employees of FWUBs. This is consistent with constitutional limits placed on federal legislation but “covers a very limited subset of the Canadian economy” because “(t)he vast majority of employers” are provincially-regulated.⁵¹
31. The Governor in Council of Canada (“GiC”) may, where satisfied that PT legislation is “substantially similar” to PIPEDA, Part 1 (pursuant to Industry Canada’s test⁵²) exempt entities other than FWUBs from its application to collecting, using, and disclosing personal information *within the PT*.⁵³ The test effectively requires PT legislation to be equivalent in terms and protection to PIPEDA and, in this sense, PIPEDA functions as a “minimum standard” for privacy protection across Canada.
32. **PT *general private sector* privacy statutes.** Some PTs have general private sector privacy legislation. The only PTs with private sector privacy statutes deemed substantially similar to PIPEDA are Alberta (“AB”), British Columbia (“BC”), and Quebec (“QC”)⁵⁴:

⁴⁷ PIPEDA s. 4(1)(a). “Commercial activities” is defined in PIPEDA s. 2(1) as “...any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.” According to OPCC, activities that “are not considered commercial” include: collecting membership fees; organizing club activities; compiling a list of members’ names and addresses; mailing newsletters; and fundraising: OPCC: How PIPEDA Applies to Charitable and Non-profit Organizations.

⁴⁸ OPCC: Commercial Activity.

⁴⁹ Voter Data and the Impact of Privacy Legislation Gaps on Cybersecurity of Elections (noting political parties are treated as exempt from PIPEDA and expressly excluded from the Privacy Act).

⁵⁰ See e.g., Churches and the Federal Privacy Law (“The reason for the commercial activity connection is that the Federal Government is relying upon its constitutional jurisdiction over general trade and commerce in Canada to implement PIPEDA. It can use this power to regulate commerce generally, but is not able to regulate the non-profit sector using this power except to the extent that the non-profit organization actually is engaged in commercial activity.”)

⁵¹GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act.

⁵² In August 2002, Industry Canada (now ISED) published the “Process for the Determination of ‘Substantially Similar’ Provincial Legislation by the Governor in Council”, outlining the policy and criteria used to determine whether PT legislation will be considered substantially similar: provide privacy protection that is consistent with and equivalent to PIPEDA; incorporate the 10 principles in Schedule 1 of PIPEDA; provide for an independent and effective oversight and redress mechanism with powers to investigate; and restrict collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

⁵³ Declaration of PHIPA as Substantially Similar to PIPEDA; Canada: Cybersecurity Comparative Guide (emphasis added) (“Under Section 26.2(b) of PIPEDA, if a province’s legislation has been deemed substantially similar to Part 1 of PIPEDA, then the organisations to which provincial legislation applies may be exempt from the application of Part 1 in respect of the collection, use and disclosure of personal information *in that province*.”)

⁵⁴ Canada: Cybersecurity Comparative Guide.

- **AB:** *Personal Information Protection Act*, S.A. 2003, ch. P-6.5 (“PIPA Alberta”), deemed substantially similar and exempted from the application of PIPEDA, Part 1 by Organizations in the Province of Alberta Exemption Order (SOR/2004-219).
- **BC:** *Personal Information Protection Act*, S.B.C. 2003, ch. 63 (“PIPA BC”), deemed substantially similar and exempted from the application of PIPEDA, Part 1 by Organizations in the Province of British Columbia Exemption Order (SOR/2004-220).
- **QC:** *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., ch. P-39.1 (“Québec Privacy Act”), deemed substantially similar and exempted from the application of PIPEDA, Part 1 by Organizations in the Province of Québec Exemption Order (SOR/2003-374).

Lawyer Carole Piosevan emphasizes that: “It is still possible for an organisation to be subject to more than one privacy law, such that one part of its operations taking place within the province is governed by provincial law and another part of its operations – which might involve the transfer of information across provincial borders – is subject to PIPEDA.”⁵⁵

33. **PT health sector privacy statutes.** PT health privacy legislation applies to “health information custodians” (“custodians”), *whether or not in the course of business*, and entities that act on their behalf (“agents”), that collect, use, and disclose “personal health information”.⁵⁶ GiC may declare that PT privacy health statutes are “substantially similar” to PIPEDA, Part 1⁵⁷, thereby exempting entities from its application to collecting, using, and disclosing PHI *within the PT*.⁵⁸ The only PTs with health privacy statutes deemed substantially similar to PIPEDA are Ontario (“ON”), New Brunswick (“NB”), Newfoundland and Labrador (“NFLD + LD”), and Nova Scotia (“NS”).⁵⁹ These statutes are beyond the scope of this submission.
34. **PT employment sector privacy statutes.** PT employment sector privacy legislation applies to *provincially-regulated, private* sector employers. The only PTs with employment sector privacy statutes are AB, BC, and QC. (As noted, PIPEDA applies to *federally-regulated, private* sector employers in PTs.)

CANADIAN PRIVACY STATUTES ARE NOT RIGHTS-BASED

35. Canadian privacy statutes do not formally recognize privacy as a right in and of itself but rather, according to OPCC, “are narrowly framed as data protection statutes” that “codify a set of rules” for how covered entities “are required to handle an individual’s personal information” (aka “data protection principles” or “privacy principles”).⁶⁰ Further, Canadian privacy statutes do not define the right to privacy in its broadest sense in accordance with Supreme Court of Canada (“SCC”) jurisprudence, which effectively defines privacy

⁵⁵ Canada: Cybersecurity Comparative Guide.

⁵⁶ Declaration of PHIPA as substantially similar to PIPEDA. See also COVID-19 and Privacy: Artificial Intelligence And Contact Tracing In Combatting The Pandemic. Health information custodians include nurses, doctors, hospitals, and medical officers of health.

⁵⁷ Declaration of PHIPA as Substantially Similar to PIPEDA.

⁵⁸ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018* (noting the health privacy legislation of some PTs has been deemed substantially similar to PIPEDA and, as such, PIPEDA does not apply to businesses operating *within* those jurisdictions, other than federally-regulated businesses); Declaration of PHIPA as Substantially Similar to PIPEDA.

⁵⁹ The statutes and exemption orders are: Ontario - *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A (“PHIPA”), deemed substantially similar and exempted from the application of PIPEDA, Part 1 by Health Information Custodians in the Province of Ontario Exemption Order SOR/2005-399; New Brunswick - *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, deemed substantially similar and exempted from the application of Part 1 of PIPEDA by Personal Health Information Custodians in New Brunswick Exemption Order SOR/2011-265; Newfoundland and Labrador - *Personal Health Information Act*, SNL 2008, c P-7.01, deemed substantially similar and exempted from the application of Part 1 of PIPEDA by Personal Health Information Custodians in Newfoundland and Labrador Exemption Order SI/2012-72; and Nova Scotia - *Personal Health Information Act*, SNS 2010, c 41, deemed substantially similar and exempted from the application of Part 1 of PIPEDA by Personal Health Information Custodians in Nova Scotia Exemption Order SOR/2016-62. Regarding PHIPA: Ontario health information custodians (and their agents) are exempt from the application of PIPEDA, Part 1, to the extent they collect, use, and disclose PHI within Ontario, and must comply with PHIPA; custodians/agents that in the course of commercial activities collect, use, and disclose PHI outside Ontario – say, to GoC or other PTs – must also comply with PIPEDA Part 1; and all personal information that is not PHI continues to be governed by PIPEDA: Declaration of PHIPA as substantially similar to PIPEDA; Ontario Privacy Laws for Lawyers.

⁶⁰ A Data Privacy Day Conversation with Canada’s Privacy Commissioner (emphasizing that “[p]rivacy is much broader than data protection – although data protection seeks to participate in the protection of privacy”); OPCC Annual Report 2018-19.

as “an individual's rights to live and develop independently, free from unjustified surveillance, while still participating in the activities of a modern digital society.”⁶¹ Legal experts explain that:

“The SCC has recognized privacy to include a notion of anonymity – that one may act in public without being personally identified or subject to extensive surveillance. Recently, the SCC concluded that privacy is not an “all-or-nothing” concept and that being in a public place does not negate all expectations of privacy with respect to being observed or recorded. The SCC has also held that privacy is vital to an individual's dignity, autonomy and personal growth, and thus that protection of privacy is a prerequisite to a free and healthy democracy.”⁶²

CANADIAN PRIVACY STATUTES HAVE SIMILARITIES & DIFFERENCES

36. “The full harmonization of all privacy legislation in Canada, which many would like to see, has yet to be achieved.”⁶³ A comparison of Canadian privacy statutes reveals that they have similarities and differences:

“While there are some similarities between privacy laws across the country, there are also key differences. This includes differences in the standards for obtaining consents from individuals and the types of exemptions federal and provincial authorities and private organizations might look for. There is not, for example, a common framework like there is in the European Union under the GDPR which contains specific exemptions for processing data including when processing is necessary for reasons of substantial public interest and specific exemptions for health data.”⁶⁴

37. In particular, Canadian private sector privacy statutes differ, between PIPEDA and PT statutes, and between the statutes of different PTs. These differences are not only substantive, but also pertain to scope/application and enforcement. For example: PIPEDA applies to private organizations in the course of commercial activities whereas PIPA AB, PIPA BC, and the Quebec Privacy Act also apply in the course of non-commercial activities; and the Quebec Privacy Act applies to personal health information, whereas PIPA AB and PIPA BC do not.⁶⁵

38. Notwithstanding these statutory differences, it is possible to identify key privacy principles and rights that individuals have in relation to the processing of their personal data (“individual rights”) (collectively, “privacy protections”)⁶⁶ (see details below).

PERSONAL INFORMATION IS SUBJECT TO MULTIPLE, COMPLEX, OVERLAPPING & INCONSISTENT CANADIAN PRIVACY STATUTES & WHEN MORE THAN ONE APPLIES YOU MUST COMPLY WITH ALL

39. The foregoing discussion demonstrates that many layers of Canadian privacy law and administrators play a concurrent, intersecting, and sometimes conflicting role. It follows that personal information is subject to:

- myriad, complex, overlapping, and inconsistent FPT privacy laws (especially privacy legislation, which is the focus of this submission); and
- multiple privacy regulators (especially privacy commissioners), with potentially multiple and overlapping investigations and enforcement proceedings for privacy violations.

⁶¹ Canada: Modernizing Federal Privacy Laws: Suggested Approaches of The Federal Government and the OPC.

⁶² Canada: Modernizing Federal Privacy Laws: Suggested Approaches of the Federal Government and the OPC. See also Privacy Commissioner of Canada Argues for Rights-based Privacy Laws in Annual Report (“For example, in *R. v. Spencer*, the Court recognized the concept of privacy as anonymity, which ostensibly facilitates the freedom to act while preserving freedom from identification and surveillance. In *R. v. Jones*, the Court affirmed that personal privacy is important to individual dignity, autonomy, and personal growth, and stated that protecting personal privacy is critical to a free and healthy democracy. Most recently, the Court in *R. v. Jarvis* held that an expectation of privacy is not necessarily unreasonable because an individual is in a public place.”)

⁶³ Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business.

⁶⁴ COVID-19 and Privacy: Artificial Intelligence and Contact Tracing in Combatting the Pandemic.

⁶⁵ Gowling: Guide to Doing Business in Canada: Privacy Law.

⁶⁶ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018* (referencing PIPEDA and PIPA AB).

40. Indeed, more than one Canadian privacy statute could and often does apply to a given organization (public or private) and OPCC stresses that: “When more than one law applies, you must comply with both”⁶⁷.
41. Further, the only way to determine what FPT privacy law(s) apply to personal information in a given situation (e.g., in context of a particular type of digital technology, such as DCTT deployed to combat the COVID-19 pandemic) is to conduct a comprehensive data flow analysis that identifies all of the entities collecting, using, and disclosing personal information and their respective roles and responsibilities. This task is further complicated in the case of digital technology owned/operated by GoC, in light of “the federal government’s publicly stated goal of moving towards a ‘tell us once’ service delivery model, where data entered in one government system can be reused by multiple other government systems”.⁶⁸

HEART OF PRIVACY LAW IS PRIVACY PRINCIPLES & INDIVIDUAL RIGHTS (“PRIVACY PROTECTIONS”)

42. The heart of privacy law is privacy protections, specifically privacy principles⁶⁹ and individual rights, which are outlined at a very high level here. First, however, it is important to identify key privacy terms.
43. **Key privacy terms.**⁷⁰ As noted, Canadian privacy law protects the use, collection, and disclosure of personal information. A working definition of these and associated terms pursuant to Canadian privacy statutes, as well as terms generally used abroad, is helpful, especially for international comparison purposes:
- **“Processing”:** Generally, not expressly defined under Canadian privacy statutes. In practice, processing includes collecting, using, modifying, storing, disclosing, or destroying personal data.
 - **“Processor” and “controller”:** Generally, not expressly defined under Canadian privacy statutes, which refer to “organizations” more broadly (including “data processors” and “data controllers”, as so defined under European privacy law (GDPR)).⁷¹
 - **“Data subject”:** Generally, not expressly defined under Canadian privacy statutes, which refer to “individuals”.⁷²
 - **“Data breach”:** Generally, not expressly defined under Canadian privacy statutes. However, some refer to “breach of security safeguards”⁷³ or a similar term, effectively defined as *loss of, unauthorized access to, or unauthorized disclosure of* personal data resulting from a breach of an organization’s safeguards or failure to establish those safeguards.
 - **“Sensitive personal data”:** Generally, not expressly defined under Canadian privacy statutes. PIPEDA provides that “any information can be sensitive, depending on the context”⁷⁴ and, as noted, personal health data is *always* regarded as “sensitive” thereunder⁷⁵.
44. As noted, despite their differences, Canadian privacy statutes have common privacy protections. This section outlines the key privacy protections (and privacy exceptions) under Canadian *private sector* privacy statutes (hence “organizations” is synonymous with “businesses” and, by corollary, government institutions are excluded unless noted otherwise). For privacy protections specific to PIPEDA, see below.

⁶⁷ OPCC: Provincial Laws that May Apply Instead of PIPEDA.

⁶⁸ OPCC Annual Report 2018-19.

⁶⁹ “Privacy principles” rather than “organization obligations” is intentional because it is accurate. As explored in greater detail below, existing privacy principles “are, in some cases, best practices rather than requirements”: OPCC Annual Report 2019-20.

⁷⁰ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 55.

⁷¹ Under GDPR, “data controller” is any *natural or legal* person that determines the means and purposes of data processing and “data processor” is any *natural or legal* person that processes personal data on behalf of the data controller: Key Features of the GDPR.

⁷² Under GDPR, “data subject” is a *natural* person whose personal data is being stored, handled or processed: Key Features of the GDPR.

⁷³ See e.g., PIPEDA s. 10.1 (1) (“An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.”)

⁷⁴ PIPEDA principle 4.3.4 (“The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information [for example, medical records and income records] is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.”).

⁷⁵ See PIPEDA principle 4.3.4 (above) as well as 4.3.6, 4.7, 4.7.2 and 4.9.1. There is significant OPCC guidance and findings on sensitivity in various contexts, and health is always sensitive.

PRIVACY PRINCIPLES

45. The key privacy principles (and exceptions) under Canadian private sector privacy statutes are the following.⁷⁶
46. **Transparency/openness.**⁷⁷ Organisations must document and make available information about their policies and practices related to managing personal data. PIAC notes that this obligation, effectively, is to *notify* individuals, who thereby gain *knowledge*, about the collection, use, and disclosure of their personal information.
47. **Lawful basis for processing (consent).**⁷⁸ Organizations must *obtain consent* to collect, use, and disclose personal data, subject to limited exceptions. Consent must be:
 - *valid and meaningful* (reasonable expectation that nature, purpose, and consequences are understood);
 - limited to fulfilling an explicitly specified and legitimate *purpose*;
 - obtained by fair and lawful *means*;
 - in a *form* – express/explicit, implied/implicit, or deemed⁷⁹ – that depends on the data’s nature and individuals’ reasonable expectations (as noted, under PIPEDA, personal health data is always regarded as “sensitive” and therefore attracts requirements of explicit consent to any collection, use, or disclosure⁸⁰); and
 - capable of *withdrawal* at any time (subject to legal or contractual restrictions and reasonable notice). Upon withdrawal, organizations must inform individuals of its implications.
48. **Purpose limitation.**⁸¹ Organizations must identify *purpose(s)* for which personal data is *collected*, at or before the collection time (“primary purpose[s]”), document such purposes in accordance with the transparency principle, and not use or disclose the data for other purposes (“secondary purposes”) except with consent or as required by law. See also data minimisation and proportionality principles.
49. **Data minimization.**⁸² Organizations must *collect, use, and disclose* personal data only to the extent (in type and volume), and *retain* it only as long as, necessary to fulfill the identified purpose(s).
50. **Proportionality.**⁸³ Organizations must only *collect, use, and disclose* personal data for *purposes* that reasonable individuals would consider appropriate in the circumstances. This principle is built into some of the others, such as the purpose limitation, safeguarding principle, and accuracy principle.
51. **Retention (and deletion).**⁸⁴ Organizations must *retain* personal data only as long as necessary to fulfil the purpose(s) for which it was collected (except for valid legal requirements), *destroy, erase, or anonymize* it when it is no longer needed to fulfill the purpose(s), and *make guidelines and implement procedures* about retention (e.g., minimum/maximum retention periods and destruction processes). See also data minimisation principle.
52. **Accountability.**⁸⁵ Organizations must *protect* (“safeguard”) personal data that is under their control – including when it is transferred to third parties for processing (“third-party processors”), at a comparable level of protection, through contractual or other means – designate a person to be accountable for the

⁷⁶ The principles that serve as the basis for Canadian private sector privacy statutes are the Canadian Standards Association’s (“CSA”) privacy principles, based on the OECD Guidelines.

⁷⁷ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 55.

⁷⁸ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, pp. 55-56.

⁷⁹ For different types of consent and their definitions, see Part 4.

⁸⁰ Health data requires explicit consent except for very rare exceptions, notably the exception for telling someone their relative is in hospital in PIPEDA s. 7.

⁸¹ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 55.

⁸² Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 55.

⁸³ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, pp. 55-66.

⁸⁴ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

⁸⁵ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, pp. 56, 58.

organisation's compliance with all privacy principles⁸⁶ (e.g., Chief Privacy Officer), and implement those principles in policies ("privacy policies") and practices ("privacy practices").

53. **Safeguarding.**⁸⁷ Organizations must *safeguard* personal data that is under their control – including data that is transferred to third-party processors (see above) – by implementing reasonable measures (technical, physical, and administrative) to protect it against loss, theft, and unauthorized access, copying, use, disclosure, change, or destruction. The more sensitive the data, the higher the level of protection required.
54. **Accuracy.**⁸⁸ Organizations must ensure personal data in their records is accurate, complete, and current, especially when it is used to make a decision about the individual or it is likely to be disclosed to a third party.
55. The "overarching rule" is "**the standard of reasonableness**", which cannot be avoided by an organization obtaining consent to an objectively unreasonable collection, use, or disclosure of personal information.⁸⁹

INDIVIDUAL RIGHTS

56. Individual rights to personal data in the custody of covered entities "recognize an essential element of privacy: that individuals retain interests in the personal information they share with others and that – rather than exercise absolute dominion over this information – the (entities) that receive it exercise shared control over (it)."⁹⁰ The key individual rights under Canadian private sector privacy statutes (and exceptions to/omissions thereof) are the following.⁹¹
57. **Right to withdraw consent.**⁹² As noted, there is a right to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and individuals must be informed of the implications.
58. **Right of access to data/copies of data.**⁹³ Organizations must, subject to limited exceptions⁹⁴, upon request, inform individuals of the *existence, use, and disclosure* of their personal data, give them *access* to it, and *provide a list* of third parties it was shared with, within a prescribed time limit or reasonable period, at no or minimal cost, and in a generally understandable form.
59. **Right to rectification of errors.**⁹⁵ When individuals demonstrate their personal data is inaccurate or incomplete, organizations generally must correct it or add a notation.
60. **Right to data portability.**⁹⁶ There is no right to data portability.
61. **Right to deletion/right to be forgotten.**⁹⁷ There is no right to require organizations to "erase" or delete personal data. (However, as noted, there is an individual right to withdraw consent.)
62. **Right to object to, or restrict, processing.**⁹⁸ There is no right to object to, or restrict, processing of personal data. However, organizations are prohibited to require – as a condition for providing a product (good or

⁸⁶ No particular title is required, however common titles include Chief Privacy Officer or Privacy Officer: Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 57.

⁸⁷ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, pp. 56, 61.

⁸⁸ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

⁸⁹ Gowling: Guide to Doing Business in Canada: Privacy Law. This can also be described as a contextual reasonable person test of appropriateness of personal information handling and protection. See PIPEDA, subs. 5(3): "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

⁹⁰ Brookings Report, *Bridging the Gaps: a Path Forward To Federal Privacy Legislation*, p. 63.

⁹¹ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018* (referencing PIPEDA and PIPA AB). Pending the outcomes of ongoing FPT privacy legislation reform efforts, new individual rights could be introduced (see details below).

⁹² Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

⁹³ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

⁹⁴ Exceptions vary across statutes (e.g., data subject to solicitor-client or litigation privilege; confidential commercial information; information about another individual; information related to national security; and information from a formal dispute resolution process): Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

⁹⁵ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

⁹⁶ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

⁹⁷ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

⁹⁸ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

service) – consent to collect, use, or disclose personal data beyond what is needed to fulfill the specified purpose.

63. **Right to object to marketing.**⁹⁹ Consent is required to collect, use, or disclose personal data for *marketing purposes*. The required *form* of consent (opt-in or opt-out) depends on the circumstances, data sensitivity, and reasonable expectations of the individual. If opt-out, conditions must be met (e.g., make individual aware of marketing purposes at or before time of collection, opt-out that is easy, immediately effective and persistent, and asap destruction or de-identification of data collected and used). Electronic direct marketing (e.g., email or SMS) is also subject to requirements under Canada’s anti-spam legislation (“CASL”) (enforced by CRTC) whereas telephone marketing is also subject to CRTC’s *Unsolicited Telecommunications Rules*, which include requirements related to the National Do-Not-Call List (“National DNCL”).
64. **Right to complain to relevant data protection authority(ies).**¹⁰⁰ There is a right to complain to the relevant data authority and, prior to this, to the organization’s designated person with accountability for its privacy compliance. Organizations must have easy-access and simple-use procedures to respond to complaints and take steps to effectively address them.

CONTEXT #2: CANADIAN PRIVACY LAW REFORM IS URGENTLY NEEDED, TO BRIDGE DIGITAL PRIVACY GAP & ENSURE MAINTAINED EU “ADEQUACY” STATUS PURSUANT TO GDPR

65. Canadian privacy law reform is urgently needed, to bridge gaps in privacy protections pertaining to digital technologies (“digital privacy gap”) and ensure that Canada maintains its status “as a country that provides ‘adequate protection’ for personal data in order to facilitate cross-border data flow between the EU and Canada”¹⁰¹ (EU “adequacy” status).

CANADIAN PRIVACY LAW REFORM IS URGENTLY NEEDED, TO BRIDGE THE DIGITAL PRIVACY GAP

66. The environment for Canadian privacy laws has changed drastically over the last two decades, especially since PIPEDA came fully into force in January 2004 and was “considered a leader among data protection legislation because of its technology-neutral, principled-based approach”¹⁰², due to rapidly evolving digital technology and its role in the growing global digital economy, which is increasingly dependent on personal information and its trade/flow within and between countries.
67. Although Canadian privacy statutes have been reviewed and revised to some degree in the interim, they are generally significantly outdated and thus unable to effectively respond to the challenges posed by the current collection, use, and disclosure of personal data in “the era of ‘big data’”¹⁰³ (aka “the new oil” and “lifeblood of today’s digital world”¹⁰⁴) by organizations – public and private – that are headquartered in Canada and other countries.
68. Concern about the digital privacy gap has been expressed by FPT commissioners and the Ontario government. For example, according to Canadian Privacy Commissioner Daniel Therrien, as of fall 2020¹⁰⁵:
 - Digital technologies “at the heart of the fourth industrial revolution” – including those that “serve the public interest, such as “crisis management” during the current COVID-19 pandemic – are beneficial but also “pose major risks to privacy” (e.g., data breaches, which “affected 30 million Canadians last year”).

⁹⁹ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, pp. 56, 58.

¹⁰⁰ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 56.

¹⁰¹ Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy.

¹⁰² The Case for Reforming the Personal Information Protection and Electronic Documents Act.

¹⁰³ The Case for Reforming the Personal Information Protection and Electronic Documents Act. “Big data” means “extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions”: Oxford Languages.

¹⁰⁴ Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*.

¹⁰⁵ September 2020 OPCC Appearance on Quebec’s Bill 64; News Release: Commissioner’s Annual Report: Pandemic Raises Privacy Concerns Highlighting Urgency of Law Reform; Remarks by Privacy Commissioner of Canada regarding his 2019-2020 Annual Report to Parliament; OPCC Annual Report 2019-20.

- These privacy risks are “not properly mitigated” by existing Canadian privacy statutes – “our existing legislative framework for privacy is outdated and does not sufficiently deal with the digital environment to ensure appropriate regulation of new technologies” and in particular “federal laws are simply not up to protecting our rights in a digital environment” – and “(t)his year, the COVID-19 pandemic makes the significant gaps in our legislative framework all the more striking”.
- For this reason, “the public no longer trusts that new technologies are being used in a way that respects their privacy”, with surveys conducted by OPCC indicating that “some 90% of Canadians are concerned about this issue” and “(o)nly 38% believe businesses respect their privacy rights, while just 55% believe government respects their privacy”.

Similarly, the Ontario consultation paper¹⁰⁶ asserts:

- Public confidence in privacy has been undermined by evolving digital technologies that collect increasing amounts and types of personal data (e.g., physical location, personal communications, and consumer preferences).
- Lack of public trust in the collection, use, and disclosure of personal data is a “barrier to adoption and effective use” of digital technologies and services.
- The “urgent need” for trustworthy digital technologies and services is highlighted by the ongoing COVID-19 pandemic.

69. A detailed overview of the digital privacy gap in Canadian privacy legislation from the perspective of Canadian consumer-citizens is provided in the PIAC Position Paper on DCTT and Privacy. PIAC believes the digital privacy gap is particularly problematic and pernicious in a world that is increasingly permeated by *surveillance capitalism* and *government surveillance* – involving indiscriminate, uncontrolled dossier/metadata/database creation on individuals, with different motives but a shared aim to subjugate the populace – wherein privacy risks also pose significant risks to respect for human individuals (call it “dignity” or “autonomy” or “democracy”).¹⁰⁷ These risks were most recently demonstrated by the Facebook/Cambridge Analytica scandal.
70. **PIPEDA’s digital privacy gap.** Among the most significant digital privacy gaps in PIPEDA are its lack of real enforcement mechanisms and its grey areas around consent, which have become muddier in the age of big data as increasingly complex information flows undermine people’s ability to fully understand what they are agreeing to.
71. **To bridge the digital privacy gap, Canadian privacy law reform is urgently needed.** To bridge the digital privacy gap, Canadian privacy law – specifically statutory – reform is urgently needed. In the October 2020 words of Canadian Privacy Commissioner Therrien, there is an “imperative need to reform our legislation”.¹⁰⁸
72. **Stop-gap measures by privacy regulators and courts are toothless.** In the absence of statutory reform, privacy regulators and courts “have increasingly had to adapt aging data protection laws to fit an ever-changing world for which they simply were not designed”.¹⁰⁹ FPT privacy commissioners have responded to the digital privacy gap by issuing collective and individual guidance on privacy and digital technology¹¹⁰, overall (e.g., May 2018 “Guidelines for Obtaining Meaningful Consent” jointly issued by OPCC and the AB and BC Privacy Commissioners) and technology-specific (e.g., guidelines on devices [digital, smart, and Internet of Things], mobile apps [overall and COVID-19 contact tracing apps], metadata, online tracking/cookies, online learning, and video games). However, since guidance is non-binding and

¹⁰⁶ Ontario consultation paper, p. 2.

¹⁰⁷ That said, for our legal conception of privacy, we will use the “Spencerian” framework for now: see *R. v. Spencer*, [2014] 2 SCR 212, 2014 SCC 43. It is the Supreme Court of Canada’s longest discussion of privacy, after all. We realize other conceptions may be possible, coming from fields such as ethics and public policy.

¹⁰⁸ OPCC Annual Report 2019-20. See also September 2020 OPCC Appearance on Quebec’s Bill 64 (stating there is “a pressing need to modernize legislation” and “case for immediate reform of the legislative framework”).

¹⁰⁹ Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*.

¹¹⁰ See e.g., OPCC Annual Report 2019-20 (noting its COVID-19 guidance documents were issued “in recognition of the fact that our laws do not provide an effective level of protection suited to the digital environment”).

unenforceable in general and, in particular, “(s)ome of the principles put forth in our guidance documents are not legal requirements”¹¹¹, it is a “stop-gap” measure without any teeth.

CANADIAN PRIVACY LAW REFORM IS DRIVEN BY GDPR, THE NEW GLOBAL STANDARD FOR PRIVACY PROTECTION

73. Canadian privacy law reform is also driven by international policy and legal developments, especially by GDPR, the new global standard for privacy protection, whose importance “is difficult to overstate”¹¹².

GDPR OVERVIEW: APPLICATION, OVERSIGHT, “ADEQUACY” DECISION/ASSESSMENT & KEY FEATURES

74. **Application and oversight.**¹¹³ GDPR applies to the private and public sector, harmonizes national data privacy laws throughout the EU, and is overseen by the European Data Protection Board (“EDPB”), comprised of representatives of the national data protection authorities (“DPAs”) and the European Data Protection Supervisor (“EDPS”). With respect to the private sector, GDPR applies to EU-established businesses and, extra-territorially, to businesses based in non-EU countries (e.g., Canada) that provide products (i.e., goods and services) to EU residents.
75. **Adequacy decisions and assessment.**¹¹⁴ In 1995, the EU adopted Directive 95/46/EC (“EU Data Protection Directive”), which pursuant to Article 25 prohibits member states (and businesses within them) from transferring personal data to a non-member state with a domestic privacy law regime that is not “adequate”. The European Commission (“EC”) has the power to determine, on the basis of Article 45 of Regulation (EU) 2016/679, whether a non-EU country offers an “adequate level” of data protection. An adequacy decision means that personal data can flow from the EU to the non-EU country “without any further safeguard being necessary” (e.g., transfer authorization – see details below).
76. The EC has recognized Canada (businesses) as providing adequate protection. Specifically, in December 2001, the EC issued Decision 2002/2/EC, which states that Canada is considered as providing an adequate level of protection of personal data transferred from the EU to recipients subject to PIPEDA (“Adequacy Decision”). Since this decision applies only to businesses subject to PIPEDA, it is referred to as a “partial” adequacy designation.¹¹⁵ The Adequacy Decision was reaffirmed in 2006, and GDPR provides for the continuity of existing EU adequacy decisions, including Canada’s.
77. The EC’s pre-GDPR monitoring obligation was reaffirmed in May 2018 through the application of GDPR Article 45(4), which requires the Commission to monitor privacy-related developments in Canada that could impact the Adequacy Decision. This monitoring activity continues as part of the GDPR evaluation and review – including examination of existing adequacy decisions – which occurs every four years, beginning in May 2020 (“EU adequacy assessment”). All countries in the “league of the adequate”, including Canada, will have their adequacy decisions reviewed by 2022.¹¹⁶ The EU adequacy assessment also applies to Canada’s PT privacy legislation.
78. In this context, the *necessary and unavoidable* question for Canadian FPT governments is what changes (if any) to FPT privacy legislation are required in order to maintain Canada’s adequacy status under GDPR and, if it is decided that such changes are not in Canada’s best interest, to develop “an alternate mechanism to

¹¹¹ OPCC Annual Report 2019-20 (justifying their inclusion on grounds they “are considered internationally to be fundamental privacy protective measures”).

¹¹² Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*.

¹¹³ Adequacy Decisions: How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection; Trade Commissioner: The European Union’s General Data Protection Regulation; Provincial Privacy Refresher Underway in Ontario.

¹¹⁴ Adequacy Decisions: How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection; Trade Commissioner: The European Union’s General Data Protection Regulation; Sixth Update Report on Developments in Data Protection Law in Canada: Report to the European Commission December 2019; Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy.

¹¹⁵ GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act.

¹¹⁶ ‘Schrems II’: Impact on Data Flows with Canada.


allows for the seamless transfer of data between Canada and the EU”¹¹⁷ (which alternate mechanism PIAC opposes). According to the EDPS, the applicable “adequacy standard” is for non-EU privacy protections to be “essentially the equivalent”¹¹⁸ of GDPR (“essential equivalence standard”) rather than a point-by-point mapping.

79. **Key features.** As noted, GDPR significantly strengthened privacy protections in the EU. From PIAC’s perspective, the most important aspect of GDPR is its emphasis on individual privacy rights and their enforcement against businesses and governments.


GDPR IS NEW GLOBAL STANDARD FOR PRIVACY PROTECTION

80. The Ontario consultation paper correctly refers to GDPR as the “new global standard” in recognition that many foreign jurisdictions – national and sub-national – have revised their privacy legislative frameworks to align with GDPR.¹¹⁹ Key examples are provided in the Table¹²⁰ below, demonstrating that Canada (federally) is a notable outlier¹²¹.

Table: Privacy Protection – Canada and Its Trading Partners (OPCC, October 8, 2020)

Jurisdiction	Year privacy law last updated	Defining privacy as a human right	Rule-making authority	Demonstrable accountability	Order-making powers	Administrative monetary penalties	Private right of action
 Canada (PIPEDA)	2015	X	X	X	X	X	X*
Argentina	2018	✓	✓	✓	✓	✓	✓
Brazil	2018	✓	✓	✓	✓	✓	✓
European Union	2018	✓	✓	✓	✓	✓	✓
United Kingdom	2018	✓	✓	✓	✓	✓	✓
Australia	2012	✓	✓	✓	✓	✓	✓
Mexico	2016	✓	✓	✓	✓	✓	X
South Korea	2018	✓	✓	✓	✓	✓	X
New Zealand	2020	✓	✓	✓	✓	X	X
Singapore	2012	X	✓	✓	✓	✓	✓
Japan	2015	X	✓	✓	✓	✓	X
California (California Consumer Protection Act)	2019	X	✓	X	X	✓	✓

✓ = yes X = no
 * The *Personal Information Protection and Electronic Documents Act* (PIPEDA) currently provides for a right for individuals to bring an organization to the Federal Court to seek remedies such as an order requiring the organization to correct its practices and/or damages, but only following an investigation and report of findings, or notice of discontinuance by the Office of the Privacy Commissioner of Canada (OPC).

 Office of the Privacy Commissioner of Canada
 Commissariat à la protection de la vie privée du Canada

81. Other countries with existing adequacy decisions (e.g., Switzerland) are in the process of updating their domestic privacy legislation to align with GDPR to ensure that when their adequacy decisions are reviewed

¹¹⁷ Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy (citing EDPS).

¹¹⁸ Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy.

¹¹⁹ Ontario consultation paper, p. 3.

¹²⁰ OPCC 2019-20, defining terms as follows: “Defining privacy as a human right”: legislation recognizes privacy as a human right, or adherence to an international agreement that does so (e.g., Convention 108); “Rule-making authority”: data protection authority or other public authority can issue enforceable codes of conduct, standards, guidance and/or regulation; “Demonstrable accountability”: data protection authority can legally seek production of specific records to prove data management practices, prior to investigation, and/or data protection authority has legal authority to conduct proactive inspections, reviews, audits to verify compliance, absent specific grounds to suspect or believe a specific infraction has occurred; “Order-making powers”: data protection authority has the power to back findings with orders for particular remedies; “Private right of action”: legal provisions allowing individuals to directly seek remedies and/or compensation from a court for breaches of privacy laws.

¹²¹ The last major revision to PIPEDA was in June 2015, via the *Digital Privacy Act*, which includes specifications on what constitutes valid consent, new exceptions to consent, new rules on breach reporting, and enhanced powers for the Canadian Privacy Commissioner (compliance agreements and broadened public interest disclosures).

there will be no need for additional safeguards to enable continued bilateral data flows.¹²² Still others are seeking new adequacy decisions (e.g., Japan).

82. It is also possible that GDPR will become the basis of an eventual multilateral privacy treaty.

CANADIAN PRIVACY LEGISLATION NOT ALIGNED WITH GDPR & SPECTRE OF “ADEQUACY” CHALLENGE LOOMS LARGE

83. **Non-alignment with GDPR.** Canadian privacy legislation, public and private sector, generally does not align with GDPR (“adequacy gaps”), a disjoint that has been described by McCarthy Tétrault LLP as “the status quo of ‘toothless’ Canadian privacy regulations” compared to “GDPR’s lofty standards”.¹²³ This is particularly true for PIPEDA (see details below).
84. **Spectre of “adequacy” challenge looms large.** Canada faces pressure to align its privacy regime with GDPR due to the spectre of an “adequacy” challenge (i.e., whether PIPEDA is still “adequate” under GDPR), which looms larger due to the July 2020 “Schrems II” decision by the Court of Justice of the European Union (“CJEU”). In Schrems II, CJEU ruled the EU-US Data Protection Shield (“Privacy Shield”) – an existing EU-US *data-sharing agreement* that replaced the EU-US “Safe Harbor” invalidated in the landmark Schrems I decision – was invalid due to concerns about US surveillance.¹²⁴ Schrems II confirmed the validity of EU *Standard Contractual Clauses (“SCCs”)*, however, as a result of the CJEU decision, the Irish DPA issued a preliminary decision that Facebook might have to stop transferring data from the EU to the US pursuant to the SCCs transfer mechanism (as of Sept 11, 2020, Facebook has sought judicial review of the decision).¹²⁵
85. Prior to Schrems II, international data protection commissioners, Canadian privacy commissioners (FPT), and Parliamentary committees underlined that Canada must act to bring Canadian legislation up to the GDPR standard, to ensure continued “adequacy” status and ideally the “interoperability”¹²⁶ of Canadian statutes with GDPR and other GDPR-like regimes (including those identified in the table above). After Schrems II, privacy experts called for “serious, rather than cosmetic, reform to PIPEDA” to maintain the free flow of data between Canada and European countries.¹²⁷
86. **Negative consequence of losing “adequacy” designation.** In PIAC’s view, “crashing out” of the GDPR adequacy designation (as the US was forced to do after the Schrems I case) would have significant and long-term negative consequences, including: potential disruptions to online commerce and international relations; security issues; and downgrading Canada’s international leadership in privacy promotion and harmonization.
87. **To bridge the adequacy gaps, Canadian privacy law reform is urgently needed.** On October 8, 2020, Canadian Privacy Commissioner Therrien noted the EU will soon be assessing Canada’s Adequacy Decision and said he thinks the country’s adequacy status is “at risk if Canada does not move” on privacy law reform, emphasizing “(t)hat in itself should be a factor for the federal government to act”.¹²⁸

¹²² The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; Switzerland – Data Protection Overview (noting the Swiss revised act is expected to enter into force by 2022).

¹²³ Provincial Privacy Refresher Underway in Ontario.

¹²⁴ Schrems II: The Saga Continues.

¹²⁵ Tech Companies Fail to Comply with New EU Regulations on Data Sharing, Survey Finds; Facebook Fights Irish Privacy Watchdog’s Data-Transfer Curbs.

¹²⁶ “Interoperability” is a concept invoked by Elizabeth Denham on behalf of the UK OIC and the international data protection commissioners, as well as by Canadian Privacy Commissioner Therrien (using it synonymously with “compatibility” in his September 2020 OPCC Appearance on Quebec’s Bill 64) and others. PIAC believes interoperability would be more persuasive and likely to be achieved if it was formally defined.

¹²⁷ The Schrems II Decision: Implications and Challenges for Canada.

¹²⁸ Commish ‘Frustrated for Canadian Citizens’ as Privacy Laws Lag.

PIPEDA v. GDPR: KEY DIFFERENCES (“ADEQUACY GAPS”)

88. A nutshell overview of PIPEDA’s adequacy gaps is pertinent here, given the Ontario privacy consultation focuses on general private sector privacy legislation. This discussion assumes a basic understanding of the current state of PIPEDA, which was described above in terms of its scope/application and shared features with other Canadian private sector privacy statutes (e.g., privacy protections). The specifics that matter here are that PIPEDA sets out ten Fair Information Principles¹²⁹ (and related sub-paragraphs) to guide private organization’s personal information handling activities and has been applied to “a wide variety” of commercial activities, including in the context of trans-border data flows”.¹³⁰

SCOPE/APPLICATION

89. **Overall.** GDPR has broad scope/application, whereas PIPEDA’s is more limited, for reasons including the following.
90. **Covered information.**¹³¹ GDPR applies to “personal data”, expansively defined as any information relating to an *identified or identifiable* individual; an identifiable individual is one who can be identified – directly or indirectly – in particular by reference to an identifier including a name, identification number, location data, online identifier (e.g., IP address or cookie ID), or factors specific to cultural, economic, genetic, mental, physical, physiological, or social identity. Employee data and business contact information are included. PIPEDA, as noted, applies to “personal information”, defined as “information about an identifiable individual”, except “business contact information” (only when used to communicate for business purposes), and employee data for non-FWUBs.
91. Personal information must be protected in a way that accounts for the form of technology and associated risks under GDPR, and be protected according to its sensitivity and level of risk under PIPEDA.¹³² GDPR designates certain types of personal data as “sensitive” (e.g., health data, information about race, ethnic origin, political opinions, religion, sexual orientation, sex life, and genetic or biometric data; criminal records are addressed separately because criminal law is outside EU’s jurisdiction) and adds extra protections for it. GDPR also permits Member States to enact specific laws, which can be stricter, about employee data. PIPEDA does not define “sensitive” personal information (driven by context).
92. **Covered entities (sectors).**¹³³ GDPR covers the private and public sectors, specifically “any natural or legal person, public authority, agency or other body that stores or processes the sensitive data of EU data subjects”.¹³⁴ It also applies “not only to targeted data collection practices, but also to the monitoring of behavior of individuals in the EU”¹³⁵ (e.g., location tracking or Internet tracking, including subsequent profiling). PIPEDA, as noted, only covers the private sector, specifically *commercial organizations* and *commercial activities* (of commercial and non-commercial organizations), albeit for constitutional reasons.

¹²⁹ The 10 Fair Information Principles, set out in PIPEDA Schedule 1, are: accountability; identifying purposes (for which PI is collected); consent (for collection, use, or disclosure of PI); limiting collection (to identified purpose); limiting use, disclosure, and retention; accuracy; safeguards; openness (about policies/practices); individual access; and challenging compliance (with Principles). For OPCC guidance (reviewed August 2020), see: PIPEDA Fair Information Principle 1 – Accountability; PIPEDA Fair Information Principle 2 – Identifying Purposes; PIPEDA Fair Information Principle 3 – Consent; PIPEDA Fair Information Principle 4 – Limiting Collection; PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention; PIPEDA Fair Information Principle 6 – Accuracy; PIPEDA Fair Information Principle 7 – Safeguards; PIPEDA Fair Information Principle 8 – Openness; PIPEDA Fair Information Principle 9 – Individual Access; and PIPEDA Fair Information Principle 10 – Challenging Compliance.

¹³⁰ PIPEDA Consultation Paper.

¹³¹ Trade Commissioner: The European Union’s General Data Protection Regulation; PIPEDA v. GDPR: The Key Differences; GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act; Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR; Chapter 5: Key Definitions – Unlocking the EU General Data Protection Regulation.

¹³² Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR.

¹³³ PIPEDA v. GDPR: The Key Differences; Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*.

¹³⁴ PIPEDA v. GDPR: The Key Differences. GDPR has different requirements for the public and private sectors, with the former granted much wider scope for use and disclosure of personal information for government purposes.

¹³⁵ PIPEDA v. GDPR: The Key Differences.

93. **Scalability.**¹³⁶ GDPR does not exclude organizations from its application based on their features (e.g., size, revenues, or amount/type of personal data) (i.e., no “applicability limits”). However, organizations are exempted from *certain obligations* based on their features (e.g., fewer than 250 employees, exempt from requirement to record processing activities). And, Recital 13 encourages Member States and their DPAs to consider the needs of small and medium enterprises (“SMEs”) and micro enterprises in applying GDPR (though many DPAs have chosen to keep their applicability criteria wide).
94. **Extraterritoriality.**¹³⁷ GDPR has “extremely broad territorial scope”¹³⁸ because it is explicitly extraterritorial (see above). PIPEDA is not explicit about whether it applies extraterritorially, however its extraterritorial application (to foreign organizations that handle Canadians’ personal information) has been upheld by Canadian courts if there is a “real and substantial” connection between the foreign organization’s activities and Canada.

PRIVACY PROTECTIONS

ORGANIZATION OBLIGATIONS

95. **Overall.**¹³⁹ GDPR has privacy *requirements* (“obligations”), thus embodying “legal drafting”. PIPEDA has privacy *principles*, thus embodying “non-legal drafting”, meaning it “contains what reads as an industry code of conduct, with some obligations but also several recommendations, examples and good practices that do not create enforceable entitlements for individuals”.¹⁴⁰ GDPR also sets out stricter but scalable obligations, meaning the level of obligations varies depending on business size/activities and personal data sensitivity/use, and certain exemptions apply.
96. **Privacy by design and privacy by default (“PbD”).**¹⁴¹ GDPR has a “(d)ata protection by design and by default” principle¹⁴², meaning that “systems and processes have to be built from the ground-up to ensure that the privacy of personal data is retained”¹⁴³, which implies “data minimisation”, meaning that only personal data absolutely necessary for the stated purpose is collected. PIPEDA does not have a PBD principle.
97. **Lawful basis/consent.**¹⁴⁴ Under GDPR and PIPEDA, organizations must have a lawful basis for collecting, using, or disclosing personal data (aka “legal basis for data processing”). A – if not the – key difference between them is the different approach to *consent* as a legal basis for data processing.
98. PIPEDA (and other Canadian *private sector* privacy legislation) is consent-based, meaning, in the words of the Ontario consultation document, that “private sector privacy laws rely on the consent of consumers as the primary enabler for the collection and use of their personal information”.¹⁴⁵ In other words, “consent is the only basis for collection, use and disclosure (with limited exceptions)”.¹⁴⁶ The “exceptions to consent”¹⁴⁷ pertain when consent would be “inappropriate” and include “publicly available information” and “journalistic purposes” exemptions, as well as other exemptions that are similar to certain GDPR alternative

¹³⁶ PIPEDA v. GDPR: The Key Differences.

¹³⁷ PIPEDA v. GDPR: The Key Differences; Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*; Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*.

¹³⁸ Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*.

¹³⁹ Trade Commissioner: The European Union’s General Data Protection Regulation.

¹⁴⁰ OPCC Annual Report 2018-19.

¹⁴¹ Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy; Key Features of the GDPR.

¹⁴² GDPR, s. 25. Technically, privacy by design and privacy by default are separate GDPR principles.

¹⁴³ Key Features of the GDPR. OPCC Annual Report 2018-19 defines PbD as “design for privacy and assess privacy risks at the start of the planning process”.

¹⁴⁴ Trade Commissioner: The European Union’s General Data Protection Regulation; PIPEDA v. GDPR: The Key Differences; GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act; The GDPR and What it Means for Canada; GDPR vs CCPA; Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR.

¹⁴⁵ Ontario consultation document, p. 4.

¹⁴⁶ GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act.

¹⁴⁷ See PIPEDA s. 7 for a list of exceptions.

bases identified below (e.g., public interest, vital interests, legal obligations). However, there is no exception for de-identified information or exception similar to other GDPR alternative bases (e.g., legitimate interests or contractual necessity).¹⁴⁸ (Note: in contrast, “[a]ll Canadian *public sector* privacy laws are based on ‘legitimate purposes’, so consent is not required where the collection, use or disclosure is lawfully authorized and legitimate”.¹⁴⁹)

99. PIPEDA s. 6.1, added in 2015, addresses valid consent, providing that: “the consent of an individual is only valid if it is *reasonable to expect* that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting” (emphasis added). Although express consent is the default, organizations can choose between “express” and “implied” consent based on specified considerations (e.g., data sensitivity and individual’s reasonable expectations). And, an organization cannot require an individual to consent to collection and use of more information than needed for purposes of a transaction to provide a product (i.e., good or service). PIPEDA does not contain a minimum age consent, however age is a factor in determining whether “informed” consent was obtained and OPCC suggests consent of children under 13 is hard to obtain.
100. Under GDPR, personal data processing is lawful if it is based on at least one of several specified “legal grounds/bases”, including but not limited to consent. These other legal grounds (i.e., “circumstances where personal data can be processed without consent”¹⁵⁰), collectively referred to as “alternative bases for lawful personal data processing” or “alternative bases to consent”, are:¹⁵¹
- “Contractual necessity”: Processing is needed in order to enter into or perform a contract with the individual.
 - “Legitimate interests”: Controller has a legitimate interest in processing, provided it is not overridden by the rights or freedoms of the individual.
 - “Public interest”: Processing is needed for tasks carried out by public authorities or organizations acting in the public interest.
 - “Vital interests”: Processing is needed to protect the individual’s “vital interests” (i.e., life-or-death situations).
 - “Legal obligations”: Controller is legally obligated to process.
101. Although consent is just one legal ground for processing personal data, it is strictly defined: it must be informed, specific, unambiguous (i.e., express not implied), and freely given, by a statement or by clear affirmative action. This definition is “so onerous that organizations will likely use it sparingly”.¹⁵² Illegal ways to obtain consent include: opt-out, implied, derived from power imbalance, and continual (e.g., when individuals change contracts or services). GDPR also contains a minimum age of consent, 16 years old, however Member States can lower it to 13-16.
102. **Derived and de-identified data.**¹⁵³ Operationally, “derived data” means information not directly supplied by individuals to an organization, including “records the organization generated internally or assembled from various sources about the individual”.¹⁵⁴ The rest of this discussion focuses on de-identified data.

¹⁴⁸ PIPEDA has a “business transaction exception”, which governs only business-business (“B2B”) transactions, not “contractual necessity” (i.e., business to individual).

¹⁴⁹ Privacy Commissioner Again Upends the Consensus on Transfers for Processing In Aggregate IQ Investigation. Put differently, legal mandate is the lawful basis for processing (aka “lawful authority-based governance model”).

¹⁵⁰ Privacy Commissioner Again Upends the Consensus on Transfers for Processing In Aggregate IQ Investigation. See also: A New Privacy Law for Ontario? (noting GDPR “sets out additional bases on which to process personal information [for example as required for the performance of a contract or for the purposes of a legitimate interest]”).

¹⁵¹ The GDPR and What it Means for Canada (bracket added); Chapter 7: Legal Basis for Processing – Unlocking the EU General Data Protection Regulation.

¹⁵² GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act.

¹⁵³ Preparing for the EU GDPR in Research Settings; Looking to Comply with GDPR? Here’s a Primer on Anonymization and Pseudonymization; Public Education Fact Sheet: De-identification and Anonymization of Personal Information.

¹⁵⁴ See e.g., Ontario consultation paper, p. 8; Torys: Ontario Enters the Private Sector Privacy Realm.

103. Since GDPR and PIPEDA only apply to “personal information”, and truly de-identified information is not considered personal information, it falls outside their scope. This begs the question of what “de-identified personal information” means. “De-identification means different things to different people” and “terminology can vary, particularly between terms such as de-identification and anonymization”.¹⁵⁵ For present purposes, PIAC defines de-identification as “the process of removing identifiers from personal information” (e.g., removing, generalizing, or replacing with a made-up alternative an individual’s names, address, date of birth, etc.) in an *attempt* to make the information no longer “about an identifiable individual” (i.e., to make it “non-personal information”).¹⁵⁶ Re-identification is “the process through which de-identified data (...) is matched back to the individual”, which can be done by combining it with identified data that is held elsewhere (e.g., publicly available or in a different database).
104. De-identification is useful to organizations (public and private) because it “supports a broad range of use cases for data”, including: internal; public release; disclosure to a third party; and **“Trusted Agent”, where “data from multiple organizations are put through a de-identification process and provided to a trusted agent (such as a data trust), which either analyzes, aggregates, or pools the data on behalf of the third party or makes it available to other parties (including the original organizations)”**¹⁵⁷. In particular, de-identified data can be “aggregated” into databases for *secondary uses/purposes* (e.g., research, performing analytics, training machine learning models, developing population insights, tracking consumer behaviour, customer segmentation, consumer profiling, and serving targeted advertisements). De-identification is frequently framed as enabling organizations to “use data for innovative purposes while simultaneously protecting and enhancing personal privacy”.¹⁵⁸
105. There are different techniques to de-identify data, including “anonymization” (personal identifiers are deleted) and “pseudonymization” (personal identifiers are replaced by artificial identifiers [“pseudonyms”]), and the difference between them rests on how likely it is for the data to be re-identified: for anonymized data, less likely and arguably impossible; and for pseudonymous data, more likely. However, there is evidence that de-identification does not work in theory or practice – there is **always** a risk of re-identification, by good and bad actors. Researchers have shown that even anonymized data can be re-identified (put differently, it is impossible for personal information to be “truly anonymized”) and that this challenge “is compounded with advances in information technology, the amount of publicly available information through online media (...) and the burgeoning and profitable data mining industry”.¹⁵⁹

*“For example, in 2006, AOL released “anonymized” search log data comprising 36 million search queries to the public. AOL suppressed identifying information such as username and IP address, yet journalists were able to link search queries back to identifiable individuals. Computer scientist Dr. Latanya Sweeney found that in the 1990 census, 87% of the American population could be uniquely identified by their combined ZIP code, date of birth and gender. More recent studies show how individuals can be linked across various online media such as social networks and blogs through their username, or how social network graphs can be analyzed to uniquely identify a user. Location data could also be used to identify an identifiable individual based on the disclosure of home and workplace locations.”*¹⁶⁰

This reality is recognized by the Canadian Anonymization Network (“CANON”), a NFP launched in May 2019 with members “comprised of large data custodians from across the public, private, and health sectors” whose “primary purpose is to promote de-identification and anonymization in Canada as privacy-respectful

¹⁵⁵ Canadian Anonymization Network: FAQ.

¹⁵⁶ Public Education Fact Sheet: De-identification and Anonymization of Personal Information. Identifiers are “both ‘direct identifiers (attributes that alone enable unique identification of an individual, such as name, address, or unique numeric identifiers) and ‘indirect identifiers’ (attributes that, when combined with other data, enable unique identification of an individual), and they can be removed/deleted or modified (to “maintain the informational value of the dataset). When identifiers are modified, “various masking techniques may be used, including, but not limited to, pseudonymization (e.g. replacing identifiers with codes), randomization (e.g., modifying attributes such that their new value differs from their true value in a random way) or aggregation (e.g. grouping values into ranges): Canadian Anonymization Network: FAQ.

¹⁵⁷ Canadian Anonymization Network: FAQ.

¹⁵⁸ Canadian Anonymization Network: FAQ.

¹⁵⁹ Public Education Fact Sheet: De-identification and Anonymization of Personal Information.

¹⁶⁰ Public Education Fact Sheet: De-identification and Anonymization of Personal Information.

means of supporting innovation and leveraging data for socially and economically beneficial purposes”.¹⁶¹ According to Canon, “the binary concept of personal information is no longer fit for purpose” because “complete anonymization for which there is virtually no risk of identifying an individual is becoming practically unattainable” and “de-identification is a relative concept that requires a contextual evaluation”¹⁶² (a point that is revisited in Part 4).

106. GDPR relaxes privacy protections for de-identified data (i.e., provides exceptions), specifically for:

- “Anonymized data”: defined as personal data with personal identifiers removed and zero re-identification risk, which is treated as non-personal data and therefore exempt from privacy protections (i.e., GDPR does not apply).
- “Pseudonymized data”: defined as personal data with personal identifiers replaced by pseudonyms and having re-identification risk if used with “additional information”, which is subject to privacy protections (i.e., GDPR applies); however, *provided the additional information is held separately*, certain obligations are relaxed.

PIPEDA does not expressly reference “de-identified” data. However, it references “anonymous” data in ways that could lead organizations to consider anonymous or de-identified data to fall outside the scope of PIPEDA.¹⁶³

107. **Data trusts.** As noted, data trusts are one type of “Trusted Agent”. “For decades, the EU has codified protections on personal data” (e.g., GDPR) and “fought against what it viewed as commercial exploitation of private information”.¹⁶⁴ However, the new European data governance strategy released by the EC in February 2020¹⁶⁵ (“European Data Strategy”), which outlines policy initiatives and investments for rollout over the next five years, takes what Canadian public policy scholar Anna Artyushina¹⁶⁶ calls a “fundamentally different approach” and “radical shift” from “protecting individual privacy to promoting data sharing as a civic duty”, by turning the EU into “an active player in facilitating the use and monetization of its citizens’ personal data”. The European Data Strategy views “data” (“personal” and “non-personal”) as a European “essential resource” and “asset” for Europe and launches an EU “single market for data” through a mechanism called “common data spaces”.¹⁶⁷ The stated purpose(s) of the EU data market is to: “ensure Europe’s global competitiveness and data sovereignty”; and “ensure that more data becomes available for use in the economy and society, while keeping companies and individuals who generate the data in control”¹⁶⁸, specifically “to encourage responsible innovation to benefit consumers and businesses”¹⁶⁹.

108. The first initiative of the European Data Strategy is the EU-funded (€7 million) “TRUSTS Project”, to be implemented by the start of 2023, which is a “consortium” that “brings together technology providers that are already deeply involved in major national data market projects” to “set up a fully operational and GDPR-compliant European Data Marketplace for *personal* related data and *non-personal* related data targeting both personal and industrial use by leveraging existing data marketplaces (...) and enriching them with new

¹⁶¹ Canadian Anonymization Network: Submission re: ISSED’s ‘Strengthening Privacy for the Digital Age’.

¹⁶² Canadian Anonymization Network: Submission re: ISSED’s ‘Strengthening Privacy for the Digital Age’.

¹⁶³ An example is Principle 4.5.3 (Limiting Use, Disclosure, and Retention), which suggests organizations should make anonymous personal information that is no longer required to fulfil the identified purposes: “Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.”

¹⁶⁴ The EU is Launching a Market for Personal Data.

¹⁶⁵ European Data Strategy. An open public consultation on the European Strategy for Data ran from February 19 to May 31, 2020, and a summary report is available at: <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-european-strategy-data>

¹⁶⁶ The EU is Launching a Market for Personal Data, by Anna Artyushina, a public policy scholar specializing in data governance and smart cities and PhD candidate in science and technology studies at York University in Toronto.

¹⁶⁷ EC: A European Strategy for Data; European Data Strategy. Note the term “data trust” is not used. The “value of the data economy” in the EU is expected to be €829 billion (5.8% of EU GDP) in 2025: European Data Strategy FAQ.

¹⁶⁸ EC: A European Strategy for Data.

¹⁶⁹ EC: Digital Finance Package: Commission Sets Out New, Ambitious Approach to Encourage Responsible Innovation to Benefit Consumers and Businesses.

functionalities and services”.¹⁷⁰ Artyushina explains that the TRUSTS Project, which currently does not enable individuals to opt-out:

“will set up a pan-European pool of personal and nonpersonal information that should become a one-stop shop for businesses and governments looking to access citizens' information.

Global technology companies will not be allowed to store or move Europeans' data. Instead, they will be required to access it via the trusts. Citizens will collect 'data dividends,' which haven't been clearly defined but could include monetary or nonmonetary payments from companies that use their personal data. With the EU's roughly 500 million citizens poised to become data sources, the trusts will create the world's largest data market.

For citizens, this means the data created by them and about them will be held in public servers and managed by data trusts. The European Commission envisions the trusts as a way to help European businesses and governments reuse and extract value from the massive amounts of data produced across the region, and to help European citizens benefit from their information. The project documentation, however, does not specify how individuals will be compensated.”¹⁷¹

109. The Ontario consultation news release recognizes that “no jurisdiction in Canada has a legislative framework for data trusts”¹⁷² (i.e., including PIPEDA).
110. **Data protection/security and breach.**¹⁷³ GDPR requires that organizations must implement reasonable data protection measures to prevent privacy breaches. PIPEDA requires organizations to adopt reasonable security safeguards (specifically technical, physical, and organizational measures), appropriate to the sensitivity of personal information (i.e., higher sensitivity means higher protection). GDPR and PIPEDA have a data breach notification requirement, requiring all breaches to be *recorded* and, if they create real risk of significant harm (“RROSH”) to an individual, to be *reported* to data protection authorities (both acts) and affected individual(s) (both acts, but for GDPR, only if there is high risk of harm to said individual’s *rights and freedoms*). However, organizations have different time frames to notify authorities (within 72 hours of awareness for GDPR and as soon as feasible for PIPEDA). GDPR refers to and defines a “personal data breach” whereas PIPEDA refers to and defines a “breach of security safeguards” and, while “(o)perationally there are few substantive differences between the definitions”¹⁷⁴, it is possible the GDPR definition is broader and makes technical failures that result in data destruction or alteration of data reportable (whereas as they are not reportable under PIPEDA).
111. **Data transfers to third parties (“outsourcing”).**¹⁷⁵ GDPR requires organizations to ensure that personal data is protected even if the data is transferred to a third-party (e.g., to a cloud provider, for storage), which means the organization is accountable for a data breach even if the third party violates the Regulation. Under PIPEDA, organizations are responsible for personal information in their custody or control, including when it is transferred to third-parties (i.e., the transferring organization remains “accountable”). PIPEDA permits outsourcing, without consent but with notice, provided the information is used for the purpose it was originally collected.
112. **Data transfers to other countries.**¹⁷⁶ GDPR imposes restrictions (conditions and safeguards) on data transfers outside the EU and, as noted, has an “adequacy” decision system, whereby cross-border transfers

¹⁷⁰ EC: Trusted Secure Data Sharing Space (emphasis added).

¹⁷¹ The EU is Launching a Market for Personal Data.

¹⁷² Ontario consultation news release, p. 3.

¹⁷³ The GDPR and What it Means for Canada; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; Trade Commissioner: The European Union’s General Data Protection Regulation; PIPEDA v. GDPR: The Key Differences; GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act; Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*. Mandatory breach reporting is a new requirement under PIPEDA, effective November 1, 2018.

¹⁷⁴ GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act.

¹⁷⁵ Trade Commissioner: The European Union’s General Data Protection Regulation; Key Features of the GDPR; Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*; OPCC: FAQ for Online Consent; Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

¹⁷⁶ Trade Commissioner: The European Union’s General Data Protection Regulation; PIPEDA v. GDPR: The Key Differences; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; GDPR vs CCPA; Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*; OPCC Annual Report 2019-20.

are restricted to countries granted an adequacy decision because they provide a comparable level of data protection (as noted, the US is not included in this list). Absent an adequacy decision, GDPR permits organizations to transfer the data if certain required safeguards (“transfer mechanisms”) are established (EC-approved Standard Contractual Clauses [“SCCs”], Binding Corporate Rules [“BCR”], or the EU-US Privacy Shield [pre-Schrems]). PIPEDA generally permits data transfers outside Canada, without consent but with notice, if the Canadian organization uses certain measures to provide a “comparable level of protection” while the data is with the foreign organization (“comparable level of protection” standard)¹⁷⁷, which “provide(s) a lower level of protection”¹⁷⁸.

113. **Data localisation.**¹⁷⁹ “Data localisation” is defined as “the legal requirement for data to be stored or processed within specific national or regional borders” and means that multi-national businesses “must establish local data storage facilities in respect of all data sourced from that country”.¹⁸⁰ According to law firm White & Case: “This trend is moving in two different directions simultaneously. In the EU, there is pressure for all such localisation requirements to be removed, to allow the truly free flow of data within the bloc. However, in a number of other parts of the world, data localisation laws are becoming increasingly popular, and in some cases are being used as a means of digital protectionism.”¹⁸¹ According to law firm Clifford Chance, as of August 2020:

“Whilst strictly there are no technical data localisation requirements under the GDPR, some critics have argued that the Schrems decisions are tantamount to de facto data localisation requirements. In the context of non-personal data, the European Commission has specifically introduced a regulation (EU) 2018/1807, effective from May 2019, which has the purpose of generally removing restrictions on the geographical limitations on the storage of data by restricting Member States from retaining or introducing new data localisation rules (...) (Globally) (i)t remains to be seen how permissively general international data transfer requirements and restrictions will be interpreted and implemented by regulators and whether these could develop into de facto localisation requirements.”¹⁸²

PIPEDA does not have a data localisation obligation.

INDIVIDUAL RIGHTS

114. **Overall.**¹⁸³ The Ontario consultation paper¹⁸⁴ emphasizes that “GDPR takes a rights-based approach to privacy protection” and “two of the most prominent of these rights relate to ‘data portability’ and ‘data erasure’”. Indeed, GDPR makes repeated references to fundamental rights of individuals in relation to data processing, throughout 173 recitals. PIPEDA is not rights-based and the specific rights to data portability and erasure do not exist within PIPEDA or Canadian privacy law.
115. **Right to withdraw consent.**¹⁸⁵ GDPR and PIPEDA grant individuals the right to withdraw consent at any time, however PIPEDA’s right has caveats (i.e., subject to legal or contractual restrictions and reasonable notice). GDPR also requires withdrawing consent to be as easy as giving it, and prohibits organizations from

¹⁷⁷ The measures are that the Canadian organization: “(i) is satisfied that the service provider has policies and processes in place to ensure that the information in its care is properly safeguarded at all times (including training for its staff and effective security measures); (ii) uses contractual or other means to “provide a comparable level of protection while the information is being processed by the third party”; (iii) has the right to audit and inspect how the third party handles and stores personal information; and (iv) at the time that the personal information is collected from an individual, makes it plain that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction”: Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA.

¹⁷⁸ OPCC Annual Report 2019-20.

¹⁷⁹ Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*; Is the Clock “Tik Toking” on Global Data Localisation?; Chapter 8: Trans-border Data Flows and Data Localization Requirements in *Big Data Law in Canada*.

¹⁸⁰ Is the Clock “Tik Toking” on Global Data Localisation?

¹⁸¹ The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020.

¹⁸² Is the Clock “Tik Toking” on Global Data Localisation? (paragraph breaks deleted, brackets and emphasis added).

¹⁸³ Trade Commissioner: The European Union’s General Data Protection Regulation.

¹⁸⁴ Ontario consultation document, p. 5.

¹⁸⁵ Trade Commissioner: The European Union’s General Data Protection Regulation; GoC’s Proposals to Modernize PIPEDA; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; Chapter 8: Consent – Unlocking the EU General Data Protection Regulation.

silently migrating to another legal basis to continue processing personal information after consent is withdrawn.

116. **Right to be informed.**¹⁸⁶ GDPR grants individuals the right to be informed about how personal data is being used. PIPEDA does not have a right to be informed.¹⁸⁷
117. **Right to access.**¹⁸⁸ GDPR and PIPEDA grant individuals the right to access personal information that organizations have collected about them.
118. **Right to rectification.**¹⁸⁹ GDPR and PIPEDA grant individuals the right to correct inaccurate personal information.
119. **Right to restrict, or object to, processing.**¹⁹⁰ GDPR grants individuals the separate rights to: restrict processing of personal data, meaning the data may only be held by the controller and only be used for limited purposes (with caveats, e.g., if the accuracy of personal data is contested); and object to processing, meaning that individuals have the right to object to processing of their personal data where the legal basis is either *public interest* or *legitimate interest*. Additionally, GDPR grants individuals specific rights to object to processing (e.g., for purposes of direct marketing and scientific, historical or statistical purposes).
120. PIPEDA does not grant a right to restrict or object to processing, however organizations are prohibited to require – as a condition for providing a product (good or service) – consent to collect, use, or disclose personal data beyond what is needed to fulfill the specified purpose.
121. **Right to be forgotten/deletion/erasure.**¹⁹¹ GDPR has an explicit right to be forgotten, which permits individuals to ask organizations to erase their personal information from their systems. The right has caveats or put differently, is “qualified” (i.e., circumstances when organizations can refuse a request) (e.g., public interest or legal obligations). Organizations are also required to inform any third-party with which they shared the personal information that a request for its erasure was made.
122. PIPEDA lacks an explicit right to be forgotten, though it is implied in provisions permitting organizations to retain personal information so long as it is needed for the purposes it was collected (implying that after that purpose is fulfilled, individuals can ask for their information to be deleted, subject to qualification [e.g., countervailing legal obligations or rights like compliance with another data retention law]). Organizations are not required to inform third-parties with whom they shared the personal information that a request for its erasure was made. Further, the scope of the (implicit) right could be limited, in that it has been argued that *de-indexing* by search engines of personal information from web search results is not commercial activity and therefore is not included¹⁹² (which could differ from a situation involving an *internal* search engine on a *commercial* website). PIPEDA also allows individuals to limit retention and require “disposal” when no longer required.
123. **Right to data portability.**¹⁹³ GDPR grants an explicit right to data portability, meaning individuals have a right to get the personal data collected on them by an organization, in a *structured, commonly used, machine-readable format* that can be easily transferred to another organization (e.g., to export contacts

¹⁸⁶ PIPEDA v. GDPR: The Key Differences; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; GDPR vs CCPA.

¹⁸⁷ However, there is a constructive right, through a filed complaint, to ask an organization to demonstrate its compliance with the *claimed* purposes, and therefore, its *actual* uses, collections, and disclosures.

¹⁸⁸ PIPEDA v. GDPR: The Key Differences; GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; GDPR vs CCPA.

¹⁸⁹ PIPEDA v. GDPR: The Key Differences; GoC’s Proposals to Modernize PIPEDA; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; GDPR vs CCPA.

¹⁹⁰ PIPEDA v. GDPR: The Key Differences; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*; GDPR vs CCPA; Chapter 9: Rights of Data Subjects – Unlocking the EU General Data Protection Regulation.

¹⁹¹ Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy; PIPEDA v. GDPR: The Key Differences; GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; GDPR vs CCPA; GoC’s Proposals to Modernize PIPEDA.

¹⁹² See details below regarding ongoing *Google Reference* case.

¹⁹³ Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy; PIPEDA v. GDPR: The Key Differences; GDPR Top Ten #1: Data Portability; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; GDPR vs CCPA.

from one online platform and transfer them to another) and, where technically feasible, will be transferred directly from one organization to another. The proviso is that the data was: provided by the individual to the organization; processed by automated means; and processed based on consent or contract fulfilment. PIPEDA has no such right.

124. **Rights related to automated decision-making and profiling.**¹⁹⁴ Rights related to automated decision-making and profiling include:

- Right not to be subject to automated decision-making and profiling: GDPR has it, PIPEDA does not.
- Right to explanation on automated decisions: GDPR has it, PIPEDA does not.

COMPLIANCE (WITH PRIVACY PROTECTIONS) & ENFORCEMENT (OF NON-COMPLIANCE)

COMPLIANCE

125. **Overall.** GDPR “raises the bar for compliance significantly”¹⁹⁵, by, as detailed above, requiring greater openness and transparency, imposing tighter limits on personal data collection, use, and disclosure, and granting individuals more, and more powerful, rights to enforce against organizations. Key additional compliance measures warrant identification here.

126. **Data Protection Impact Assessment (“DPIA”) & Compliance Reviews.**¹⁹⁶ GDPR requires a DPIA to be conducted, when initiating a new project, product or service, and when there is a significant change (e.g., new process or change to existing process) to the way personal data is processed, to pre-emptively identify privacy risks. Organizations must also conduct Compliance Reviews to ensure that identified privacy risks are addressed. PIPEDA does not require a Privacy Impact Assessment (“PIA”), never mind compliance review, to be conducted.

127. **Data protection officer (“DPO”).**¹⁹⁷ GDPR requires a DPO to be appointed by organizations that process personal data on large scale, to ensure compliance with the Regulation, and the DPO must be an expert on data protection law. PIPEDA requires organizations to appoint a data protection officer, but does not prescribe a specific title (typically called “Chief Privacy Officer” or “Privacy Officer”) or set out specific qualifications, and there are no specific sanctions for failing to appoint one.

128. **Record-keeping.**¹⁹⁸ GDPR requires comprehensive internal records of data processing activities to be kept, to demonstrate compliance. PIPEDA does not.

129. **Self-regulation mechanisms.**¹⁹⁹ GDPR encourages self-regulation mechanisms (e.g., technical and operational standards and codes and voluntary certification systems) to incent privacy-protective practices by organizations.²⁰⁰ PIPEDA “currently contemplates a role for codes of practice” but does not formally recognize “(t)he development of codes of practice, accreditation/certification schemes, and standards as a means of demonstrating due diligence in regards to compliance with certain provisions of the Act”.²⁰¹

¹⁹⁴ PIPEDA v. GDPR: The Key Differences; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy; The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020; GDPR vs CCPA.

¹⁹⁵ Chapter 1: The Rapid Evolution of Data Protection Laws, in The International Comparative Legal Guide to Data Protection 2018.

¹⁹⁶ Trade Commissioner: The European Union’s General Data Protection Regulation; Key Features of the GDPR; The GDPR and What it Means for Canada; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA.

¹⁹⁷ Trade Commissioner: The European Union’s General Data Protection Regulation; Key Features of the GDPR; Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018.

¹⁹⁸ Trade Commissioner: The European Union’s General Data Protection Regulation.

¹⁹⁹ Canadian Anonymization Network: Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’.

²⁰⁰ See e.g., GDPR Art. 42 Certification (encouraging establishment of data protection certification mechanisms for purpose of demonstrating compliance with GDPR).

²⁰¹ GoC’s Proposals to Modernize PIPEDA. Regarding current role for codes of practice, see e.g., PIPEDA s. 24(c) (“The Commissioner shall encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with Divisions 1 and 1.1”).

ENFORCEMENT

130. **Overall.**²⁰² GDPR includes strong enforcement powers and severe sanctions for non-compliance. DPA powers are: investigative (e.g., to investigate and correct any noncompliance issues and perform audits to ensure compliance); corrective (e.g., to issue warnings and reprimands, demand compliance within prescribed deadlines, order erasure of personal data or communication of data breaches, and prevent organizations from processing data); and advisory (e.g., to accredit certification bodies, adopt standard data protection clauses, and approve BCRs). Sanctions include significant financial penalties.
131. PIPEDA includes relatively weak enforcement powers and mild consequences for non-compliance. OPCC's enforcement powers are:
- **Investigative:** including to investigate complaints (self-initiated or public-initiated), refuse or discontinue complaints in certain defined circumstances, and conduct audits of data practices (for suspected non-compliance only).
 - **Corrective:** including to issue *non-binding* recommendations and public reports about an organization's privacy practices, enter compliance agreements²⁰³, and, at the end of a *public-initiated* investigation, take the matter to the Federal Court of Canada ("Federal Court"), which can order remedies or award monetary damages, including for humiliation suffered.

To achieve compliance objectives, PIPEDA primarily emphasizes mediation, negotiation, and education (the "ombudsman model"), including requiring OPCC to educate organizations and individuals about the Act, conduct research, develop guidance, and encourage development of codes of practice. The Ontario consultation paper²⁰⁴ correctly asserts that certain enforcement powers are "generally absent" from the Canadian privacy regime (e.g., to issue binding orders and impose financial penalties), including PIPEDA, thereby undermining the ability of FPT privacy commissioners to enforce compliance and encourage compliant privacy practices by organizations.

132. **Binding orders:**²⁰⁵ GDPR has binding orders, whereas PIPEDA does not. Under PIPEDA, OPCC cannot issue binding orders against organizations, and the only way to get its findings/recommendations enforced is to bring an action in Federal Court, which is only permitted for complaints the Commissioner did not initiate. Litigating a matter in Federal Court is onerous and costly for applicants, and delays the outcome of an OPCC investigation unless/until the court comes to the same conclusion.
133. **Financial penalties (overall).**²⁰⁶ Unlike PIPEDA, GDPR has "serious penalties" for non-compliance, and "appears to leave open the possibility that penalties could be applied to both controllers and processors".²⁰⁷ However, EU regulators do not view financial penalties as "front-line compliance tools" and "have indicated

²⁰² OPCC: Enforcement of PIPEDA; Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy; Ontario consultation paper, pp. 6-7; Strengthening Privacy In the Digital Age; The GDPR and What it Means for Canada; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; GDPR vs CCPA.

²⁰³ A "compliance agreement" is a voluntary agreement whereby the organization commits to comply with OPCC's recommendations and to bring itself into compliance with PIPEDA. If the organization does not meet its commitments, OPCC can apply to the Federal Court for an order to comply with the compliance agreement. A current example is OPCC's compliance agreement with Equifax Canada, which was revised in January 2020 to change certain consent requirements regarding transborder data flows: OPCC Annual Report 2019-20.

²⁰⁴ Ontario consultation paper, pp. 6-7.

²⁰⁵ PIPEDA, s. 15; Ontario consultation paper, p. 6; Privacy Commissioner of Canada Argues for Rights-based Privacy Laws in Annual Report.

²⁰⁶ Trade Commissioner: The European Union's General Data Protection Regulation; Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy; Ontario consultation paper, p. 6; Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*; Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*; The GDPR and What it Means for Canada; PIPEDA v. GDPR: The Key Differences; Key Features of the GDPR; Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA; GDPR vs CCPA; OPCC: What You Need to Know About Mandatory Reporting of Breaches of Security Safeguards; Privacy Commissioner of Canada Argues for Rights-based Privacy Laws in Annual Report.

²⁰⁷ Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*.

that they would prefer to work with businesses to ensure that GDPR compliance is achieved”.²⁰⁸ There are two key types of financial penalties, fines and statutory damages:

- **Fines:** Fines can be imposed by the government agency administering a statute for non-compliance (“civil fines”, “administrative fines/penalties/sanctions” or “administrative monetary penalties [AMPs]”) or imposed by courts, for criminal offences under a statute (“penal fines/penalties/sanctions”). GDPR and PIPEDA have fines, but GDPR’s are administrative (i.e., applied by DPAs) and bigger (up to 4% of global annual revenue or €20 million, whichever is higher).²⁰⁹ PIPEDA’s fines are penal, maximum CAD\$100,000,²¹⁰ and can be imposed by the Federal Court in a limited number of circumstances (e.g., organization retaliates against employee whistleblowers, knowingly destroys data that is subject to an ATI request, obstructs OPCC in investigating a complaint or conducting an audit, uses deception or coercion to collect data in violation of the act, or fails to notify in the event of a breach). OPCC refers information related to the potential commission of an offence to the Attorney General (“AG”) of Canada, who is responsible for any ultimate prosecution.
- **Statutory damages:** In context of a private right of action, “statutory damages” means a court-imposed damage award that is stipulated within the legislation rather than calculated based on the degree of harm to the individual (“actual damages”, which can be “general damages” or “exemplary/punitive damages”). Neither GDPR nor PIPEDA has statutory damages.²¹¹

134. **Private right of action.**²¹² A “private right of action” (aka “independent right of action”) means a right for individuals to sue non-compliant organizations in court and seek remedies, including damages (actual and/or statutory)²¹³, which can be used for non-compliance with any statutory provision or limited to certain violations. GDPR and PIPEDA have a private right of action, however GDPR’s is broader (e.g., right to “effective judicial remedy” where individual considers their rights under GDPR have been infringed, and to receive compensation for any damage, material or non-material) and PIPEDA’s is narrower (i.e., right for an individual— only after they receive an OPCC report or notice that OPCC’s investigation has been discontinued – to bring an organization to Federal Court, which can, for certain violations²¹⁴, order an organization to correct its privacy practices and/or award damages, including for “humiliation”, but limited in practice to tens of thousands of dollars)²¹⁵. Since PIPEDA allows individuals to pursue court actions *only with Commissioner involvement*, some experts refer to PIPEDA’s private right of action as a “limited private right of action”²¹⁶ whereas OPCC refuses to recognize it as a private right of action (e.g., see OPCC Table above). For ease of discussion, PIAC adopts the first usage and, therefore, refers to the “existing” private right of action

135. A private right of action can be for *individual* actions only, or also include *class* actions (aka “class proceedings”), whether expressly (i.e., legislation permits them) or through breach of contract. GDPR

²⁰⁸ Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*.

²⁰⁹ These maximum fines are for serious violations; minor violations attract a fine of €10 million or 2% of global revenue, whichever is higher.

²¹⁰ According to GoC’s Proposals to Modernize PIPEDA: “Under PIPEDA as currently drafted, there are two categories of offence: an offence punishable on summary conviction and liable to a fine not exceeding \$10,000 (per offence); an indictable offence and liable to a fine not exceeding \$100,000 — (maximum of \$100,000 per offence). These categories of offences are distinguished based on the severity of the contravention. Typically, summary offences are less serious than indictable offences. The Attorney General of Canada has the discretionary power to qualify the contravention as either type of offence depending on the nature of the contravention. Fines are applied by the Courts.”

²¹¹ Regarding PIPEDA, see e.g., Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime (“[T]here are no statutory punitive damages under PIPEDA”).

²¹² OPCC Annual Reports 2018-19 and 2019-20; OPCC: How to Apply for a Federal Court Hearing Under PIPEDA; Data Class Actions in Europe; OPC Happy With Tracing App, But Not With Privacy Law.

²¹³ See e.g., OPCC Annual Reports 2018-19 and 2019-20 (defining private right of action as “independent right of action in the courts to seek remedies for non-compliance with [individuals’] rights” and “legal provisions allowing individuals to directly seek remedies and/or compensation from a court for breaches of privacy laws”).

²¹⁴ The PIPEDA private right of action “is based specifically on the loss, misuse, or unauthorized access to personal information held by an organization”: Current Landscape of Personal Information and Privacy Liability in Canada.

²¹⁵ PIPEDA s. 16 authorizes courts to award damages, including for humiliation, arising from a statutory breach and “(o)ver the past few years there has been an evolution towards courts awarding greater damages amounts”: Canada: Putting a Dollar Figure on Breach of Privacy in Canada. In the notable case of *Chitraker v. Bell*, the court awarded damages of \$20K, comprising \$10K in general damages and \$10K in punitive damages, which as of December 2013 signified “the largest damages award to date under PIPEDA” and “the first time... punitive damages have been awarded under PIPEDA”: Damages Under PIPEDA: A Purposive Approach and a New High Water Mark.

²¹⁶ OPC Happy With Tracing App, But Not With Privacy Law.

permits collective rights of action (“data collective actions”), including a limited class action (“data class actions”), which can be brought by NFPs dedicated to personal information protection.²¹⁷ As of January 2020, according to law firm McCarthy Tétrault, it is uncertain whether PIPEDA only allows for individual actions and “(i)t is possible (...) that an independent right of action could lead to class actions through breach of contract”.²¹⁸

CONTEXT #3: CANADIAN PRIVACY LAW REFORM (FPT) IS UNDERWAY BUT WOEFULLY STALLED & FRAGMENTAL

CANADIAN PRIVACY LAW REFORM (FPT) IS UNDERWAY, SHOWING THE QUESTION IS HOW, NOT WHETHER, TO MODERNIZE PRIVACY STATUTES

136. OPCC correctly asserts that “(t)he question is no longer whether privacy laws should be modernized, but how”²¹⁹. The truth of this statement is demonstrated by the fact that Canadian privacy law reform is underway, specifically, efforts to reform private and public sector privacy legislation, at the FPT level. In particular, reform of Canadian private sector privacy statutes (FPT), especially of general application, is ongoing. A brief overview of key developments follows.
137. **FPT privacy reform (overall).** In October 2019, a Joint Resolution by FPT privacy commissioners, entitled “Effective Privacy and Access to Information Legislation in a Data Driven Society” (“October 2019 Joint Resolution by FPT Privacy Commissioners”), was issued. The resolution asserts the need to “enhance and establish consistent modernization” of information and privacy laws across Canadian jurisdictions, in order to better protect individuals.
138. **Federal privacy reform.** A federal government review of PIPEDA (and separately, of the Privacy Act [“PA”]), is ongoing.²²⁰ FPT privacy commissioners, the House of Commons Standing Committee on Access to Information, Privacy and Ethic (“ETHI”) members, from all parties, and GoC agree that PIPEDA should be *fundamentally reformed*. For example:
- **May 2019:** Canada’s Digital Charter²²¹ (“Digital Charter”) was announced²²² and Innovation, Science and Economic Development (“ISED”) proposed changes to modernize PIPEDA in a discussion paper entitled “Strengthening Privacy for the Digital Age”²²³ (aka “GoC’s Proposals to Modernize PIPEDA”), thereby initiating an open consultation. The Canadian Data Governance Standardization Collaborative was established; a final roadmap that takes a “life-cycle approach to data governance from data collection, through access and sharing and ending with data analytics and commercialization” is expected late 2020 and will be “used to facilitate greater understanding of standardization priorities for data governance in Canada”.²²⁴
 - **June 2019:** ETHI released a report on its study on privacy of digital government services (“ETHI Report”), which makes recommendations to the federal government, including to modernize PIPEDA (and the Privacy Act) by adopting the Committee’s recommendations on these acts in previous reports.²²⁵
 - **December 2019:** OPCC released its Annual Report 2018-19 to Parliament (“OPCC Annual Report 2018-19”), which “sets out a blueprint for how to modernize Canadian privacy laws”²²⁶, including

²¹⁷ Data Class Actions in Europe.

²¹⁸ Privacy Commissioner of Canada Argues for Rights-based Privacy Laws in Annual Report.

²¹⁹ OPCC Annual Report 2018-19.

²²⁰ Modernizing Canada’s Privacy Act.

²²¹ Digital Charter. See also Canada’s Digital Charter: Trust in a Digital World.

²²² Minister Bains Announces Canada’s Digital Charter.

²²³ Strengthening Privacy for the Digital Age.

²²⁴ ISED’s Sixth Update Report on Developments in Data Protection Law in Canada: Report to the European Commission December 2019.

²²⁵ Specifically: Report 4- Protecting the Privacy of Canadians: Review of the Privacy Act (December 2016); Report 12 – Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act (February 2018); Report 16 – Addressing Digital Privacy Vulnerabilities and Potential Threats to the Canadian Democratic Electoral Process (June 2018); and Report 17 – Democracy at Risk: Risks and Solutions in the Age of Disinformation and Data Monopoly (December 2018): ETHI Report.

²²⁶ OPCC News Release: Commissioner’s Annual Report Sets Out Blueprint for How to Modernize Canadian Privacy Laws.

recommendations for PIPEDA reform. Shortly afterwards, in the wake of the October 2019 federal election, PM Trudeau issued ministerial mandate letters, of which some included direction on privacy law reform. For example, the ISED Minister was mandated to advance the Digital Charter, enhanced powers for the Canadian Privacy Commissioner, and specified revisions to PIPEDA (and the Privacy Act).²²⁷

- **October 2020:** OPCC released its Annual Report 2019-20 to Parliament (“OPCC Annual Report 2019-20”), which confirms that “(t)he recommendations for legislative change set out in our 2018-2019 annual report remain extremely relevant” and “our blueprint for legislative reform”.
139. The Ontario consultation paper correctly emphasizes that GoC “has indicated its intent to modernize PIPEDA, however to date there have not been any substantial changes”.²²⁸ Strengthening Privacy for the Digital Age states that discussions resulting from it “will inform the development of options for legislative reform” and, as of March 2020, GoC has consulted with “a broad range of stakeholders (e.g., private organizations, business associations, civil society, and academia).²²⁹ However, to date, no PIPEDA legislative amendments have been introduced, delayed in part due to the ongoing COVID-19 pandemic. Meanwhile, Canada continues to participate in international fora (e.g., Organisation for Economic Co-operation and Development [“OECD”] and Asia-Pacific Economic Cooperation [“APEC”]) that are engaged in initiatives to improve and expand “the global interoperability of privacy frameworks”.²³⁰
140. The federal government is expected to be focused on COVID-19 through Fall 2020, and while certain stakeholders (e.g., Canadian Marketing Association [“CMA”]) “expect PIPEDA reform to be a high priority once the parliamentary schedule begins to return to normal” and to consist of “the most significant changes (...) in almost two decades”²³¹, this timeline and outcome is uncertain. As Canadian Privacy Commissioner Therrien stated on October 8, 2020: “The short answer is I don't know when the government will table privacy legislation. I see that a number of provinces apparently are getting weary of inaction by the federal government and are starting to act.”²³²
141. **PT privacy reform.** Certain PTs are in the process of reviewing their privacy legislation, some at an early stage (specifically BC, which in February 2020 appointed a Special Committee of the Legislative Assembly to review PIPA BC that wrapped up its consultation in August and aims to make recommendations in a report to be released by February 2021²³³) and others at a later stage (specifically, Quebec, which in June 2020 introduced amending legislation, Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*²³⁴ [“Quebec Bill 64” or “Bill 64”] proposing “sweeping reform” to strengthen the province’s existing private and public sector privacy statutes).²³⁵ Since Quebec has a majority government, it is expected that Bill 64 will be adopted, in some form, by spring-fall 2021, and since its transitional provisions provide that it will generally enter into force one year after its date of assent, most provisions are not expected to come into force until spring-fall 2022.²³⁶
142. The BC Special Committee is expected to consider whether to align PIPA BC (which does not currently have an EC adequacy decision) with PIPEDA (presumably its current iteration), other PTs’ private sector privacy statutes, and/or GDPR. In contrast, Bill 64 is widely viewed to represent a strong alignment of existing

²²⁷ December 2019 ISED Minister Mandate Letter.

²²⁸ Ontario consultation paper, p. 3.

²²⁹ ISED’s Sixth Update Report on Developments in Data Protection Law in Canada: Report to the European Commission December 2019.

²³⁰ ISED’s Sixth Update Report on Developments in Data Protection Law in Canada: Report to the European Commission December 2019.

²³¹ Privacy Update – Provincial privacy law reform, final CCPA regulations and more; Privacy Update – Provincial privacy law reform, final CCPA regulations and more.

²³² COVID-19 pandemic reveals major gaps in privacy law, says watchdog.

²³³ Legislative Assembly of British Columbia, Parliamentary Committees, Special Committee to Review the Personal Information Protection Act; Canada: Special Committee Begins Consultations On Changes To BC’s Personal Information Protection Act; A New Privacy Law for Ontario.

²³⁴ Online: <http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html> (note: includes political parties).

²³⁵ Torys: Ontario Enters the Private Sector Privacy Realm. See also: Ontario consultation paper, pp. 2-3. The acts are the *Act respecting the protection of personal information in the private sector* (“Private Sector Act”) and *Act respecting Access to documents held by public bodies and the Protection of personal information* (“Public Sector Act”). The Private Sector Act has not received an Adequacy Decision. Indeed, in 2014, the Article 29 Data Protection Working Party (“G29”) recommended to the EC *not* to declare it “adequate”: Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business.

²³⁶ Canada: Bill 64: Modernizing Québec’s Privacy Regime.

Quebec privacy legislation with GDPR. According to the former Justice Minister, Sonia LeBel, it is intended to be “very closely modeled on European best practices” and “give more teeth” to existing statutes²³⁷, and its features include new individual rights (e.g., erasure and data portability), increased enforcement powers for the Commission d’accès à l’information (“CAI” or “Quebec Commission”), hefty fines (up to \$10M or 2% of a business’ worldwide revenues), and an “adequacy” requirement that appears to target inter-PT as well as international trade. According to McMillan LLP, “(t)his modernization would arguably make Québec’s privacy regime the strictest on this side of the Atlantic”.²³⁸ According to Constantine Karbaliotis, a Toronto lawyer and expert in global privacy compliance and privacy management with virtual law firm nNovation LLP, Bill 64 “may compel the conversation that needs to be had about privacy (...) Quebec may be setting the tone for the country”.²³⁹

143. **Ontario privacy reform.** The Ontario government is proposing to create private sector privacy legislation of general application that, given the proposed Ontario rules, would be a somewhat GDPR-like Ontario statute, albeit the rules “appear to be less onerous than requirements proposed under Quebec’s Bill 64 and under the EU GDPR regime”.²⁴⁰ The Ontario privacy consultation is “a preliminary stage of the legislative process” and, if the Ontario government decides to proceed with the proposed legislation, it could be “several years” before it enters into force.²⁴¹
144. This is not the first time that Ontario has tried to introduce general private sector privacy legislation. The province attempted to enact such legislation by way of Bill 14, the *Personal Information Protection Act* (“PIPA”), a private member’s bill, introduced on the eve of an election, which had first reading on March 21, 2018, and passed second reading on March 22, 2018, but died on the Order Paper.²⁴² In 2002, a proposed statute, the *Privacy of Personal Information Act, 2002* (“PPIA”), was circulated for public comment but did not become law.²⁴³

CANADIAN PRIVACY LAW REFORM, ESPECIALLY FEDERAL, IS WOEFULLY STALLED & FRAGMENTAL

145. The foregoing discussion demonstrates that Canadian privacy law reform is, woefully, stalled and fragmental.

PART 3: PIAC’S POSITION ON CANADIAN PRIVACY LAW REFORM (OVERALL) UNDERPINS OUR RECOMMENDATION IN THIS CONSULTATION – TAKE TWO TRACK APPROACH, WITH IMMEDIATE FOCUS ON “GDPR-IZING” FEDERAL PRIVACY STATUTES & PT STATUTES IN AREAS OF PRIMARILY/EXCLUSIVELY PT JURISDICTION & LONG-TERM AIM OF UNIFIED FEDERAL PUBLIC/PRIVATE SECTOR LEGISLATION

146. PIAC’s position on Canadian privacy law reform (overall) underpins our recommendation in this consultation.

FUNDAMENTAL QUESTION THAT BEGS ASKING: IS NEW PT GENERAL PRIVATE SECTOR PRIVACY LEGISLATION (OVERALL) A STEP IN RIGHT DIRECTION?

²³⁷ OPCC Annual Report 2019-20 (citing former Justice Minister).

²³⁸ Canada: Bill 64: Modernizing Québec’s Privacy Regime.

²³⁹ Quebec Plans Ambitious Overhaul of its Privacy Law.

²⁴⁰ Provincial Privacy Refresher Underway in Ontario. See also: Ontario Government Launches Consultation to Enhance Privacy Protection (“In light of the advice being sought, it appears that the Ontario government is looking to implement a General Data Protection Regulation [GDPR]-like statute for the province of Ontario, which is consistent with the approach taken by the Quebec government in respect of Bill 64.”); Torys: Ontario Enters the Private Sector Privacy Realm.

²⁴¹ Ontario enters the private sector privacy realm.

²⁴² Canada: An Employer’s Guide To Privacy In The Workplace.

²⁴³ Canada: Ontario Tries Again – Provincial Government Launches Consultation On Strengthening Provincial Privacy Laws.

147. The Ontario privacy consultation assumes the fundamental question that begs to be asked: is new PT general private sector privacy legislation a step in the right direction? PIAC's answer, in a nutshell, is: no.
148. This PIAC view, and our Ontario-specific recommendations in this submission, are grounded on PIAC's broader position on Canadian privacy law reform (overall), which we will briefly outline next in the interest of transparency. We would be pleased to make ourselves available for any follow-up questions or discussion of the high-level points raised here.

PIAC'S ANSWER: NEW PT GENERAL PRIVATE SECTOR PRIVACY LEGISLATION IS A STEP IN WRONG DIRECTION

NEW PT GENERAL PRIVATE SECTOR PRIVACY LEGISLATION WOULD FURTHER FRAGMENT EXISTING PATCHWORK, THUS UNDERMINING PRIVACY PROTECTION FOR CANADIANS

149. PIAC's view is that **Canadians will be better protected by a strengthened federal personal information protection regime than by increasing PT-by-PT legislation and further fragmenting the existing legislative and regulatory patchwork.** It could superficially appear that better privacy protection for Canadians at any jurisdictional level, as quickly as possible, would be a positive development. The introduction of PT general private sector privacy legislation might be welcomed by those who are eager for privacy law reform and understandably frustrated being at the mercy of a slow-moving federal process to revise PIPEDA. However, there are reasons to be wary of further fragmenting privacy legislation along PT lines.
150. **Exacerbated uneven privacy protection and risk of legal gamesmanship.** Without highly coordinated pan-provincial consistency and cooperation, additional PT-by-PT enactment of general private sector privacy statutes risks providing more uneven protection to Canadians, whose personal information is already treated differently based on territorial factors like the residency of the individual, the storage location of the data, and the locus of incorporation of the business that offers the service. There's also a risk that the move will encourage legal gamesmanship, with businesses simply transferring operations to weaker privacy jurisdictions.
151. **Complicated business environment and exacerbated trade barriers.** A further fragmented patchwork of PT general private sector privacy statutes would also complicate the business environment and potentially exacerbate internal and international trade barriers. In the words of the Ontario Chamber of Commerce: "It is important that the Government of Ontario avoids duplicating federal government laws pertaining to the collection, use, and disclosure of personal information by private sector organizations. A patchwork of privacy rules would add additional costs, complicate the business environment, and act as an unnecessary barrier to interprovincial trade."²⁴⁴ The Retail Council of Canada (RCC) "is deeply concerned that provinces will try to create 'better' versions of PIPEDA, resulting in a hodgepodge of different systems that are incompatible with one another, stymying both international and inter-provincial trade and potentially putting Canadians at risk of data breaches due to confusion between different provincial and territorial regimes."²⁴⁵
152. **Increased compliance burden and consumer costs.** The movement of personal data across both national and international borders is essential to the Internet economy, and some Ontario business leaders are already balking at the increased compliance burden posed by multiple, potentially inconsistent layers of regulation. Such challenges are playing out in the US, which has begun its own state-by-state introduction of consumer privacy legislation in the void of a comprehensive national regime. Businesses are seeing that even slight inconsistencies between statutes—and even between rules that appear on the surface to grant the same rights, such as data portability—can lead to huge compliance costs, which may be passed onto consumers in the form of both higher prices and a shrunken market. Some analysts have pointed to an

²⁴⁴ Ontario's Privacy Consultation Could Lead to New Private Sector Data Protection Laws, But Not Everyone is Thrilled About It.

²⁴⁵ Submission by Retail Council of Canada to Special Committee to Review the BC Personal Information Protection Act.

emerging irony in the global privacy crackdown: rules that are outwardly pro-consumer may end up empowering the very tech monoliths whose abusive data practices they're meant to target, since these companies have the deep pockets to absorb rising compliance costs and increased legal risk. While poll after poll shows that Canadians do have an interest in strong privacy protections, a robust federal statute can avoid the unnecessary compliance burden posed by a proliferation of regional frameworks.

153. **Challenges for privacy regulators.** While promising to protect consumer-citizens within each PT, an enhanced piecemeal approach to privacy could also pose challenges for federal and PT privacy regulators. Again, we can look for guidance to the international context, where traditional notions of territoriality and jurisdictional authority are being challenged by the nature of electronic data. Even as the EU's adequacy requirement has put increasing pressure on countries to update – by GDPR-izing – their privacy laws, data privacy rights vary considerably across national borders, and the speed, ease, and complexity of global data circulation often severs the factual link between the location of data and the location of its user. This tension between bordered privacy regimes and borderless data has led to serious conflicts between countries seeking control over online information, including efforts by governments to set global privacy standards via their own domestic regulation. The result is that businesses, regulators, and consumers increasingly operate in an environment of uncertainty in which it is unclear which country's or region's laws govern online data at any given time. An increased patchwork of provincial laws risks reproducing this uncertainty within Canada.
154. **Expense for PT governments.** Managing these complexities will likely be pricey for PT governments. As former federal privacy commissioner Jennifer Stoddart notes, Quebec's Bill 64 intends to deal with the issue of cross-border transfers via a GDPR-style adequacy condition that requires assessment of the destination's privacy regulations, but this process has proved cumbersome to even the EU's large, experienced bureaucracy. In the EU, regulators are finding that the GDPR requires enormous investment and staffing resources in order to give it teeth. And in the US, state privacy laws are under near-constant amendment to close ambiguities and catch up to other jurisdictions. Even if Ontario's rules would apply only to commercial activities within the province and not to interprovincial or international transfers, there are costs involved in reviewing and assessing compliance with any new regulatory regime.
155. Those impatient for change might be reassured by the rising urgency of federal privacy reform, driven by GDPR adequacy concerns, described above. PIAC believes that a single, robust federal privacy regime is a more realistic road to adequacy and to ensuring the EU is confident exchanging data with Canada.

CANADIAN PRIVACY LAW REFORM (OVERALL) SHOULD TAKE TWO TRACK APPROACH

156. PIAC's foundational position on Canadian privacy law reform is that **FPT governments should simultaneously pursue a two-track strategy, with immediate focus on "GDPR-izing" federal privacy statutes and PT privacy statutes in areas of primarily/exclusively PT jurisdiction and the long-term aim of unified federal public/private sector legislation.** This position is detailed next.

TRACK #1: IMMEDIATE FOCUS ON "GDPR-IZING" FEDERAL PRIVACY STATUTES & PT STATUTES IN AREAS OF PRIMARY/EXCLUSIVE PT JURISDICTION

157. Pursuant to Track #1, which is short/medium term (2-4 years), PIAC **recommends** that FPT governments should:
 - *Strengthen* FPT privacy legislation, by *aligning it with GDPR* (i.e., "GDPR-ize" Canadian privacy law), to the extent possible given Canada's unique circumstances, focusing on the federal PIPEDA and Privacy Act ("PA") as the overarching models. We agree with OPCC that it is important to "avoid going beyond" GDPR, "unless (governments) deem it necessary for specific provisions".²⁴⁶

²⁴⁶ September 2020 OPCC Appearance on Quebec's Bill 64.

- Take urgent action on GDPR-izing PIPEDA. PT governments with provincial private sector privacy legislation of *general application* (existing or new) – which PIAC opposes for the reasons provided above – should aim to substantively align it with the *revised PIPEDA*, in order to avoid any unnecessary conflict between compliance regimes (federal-PT and inter-PT) and maintain “substantially similar” status to PIPEDA.
 - Concentrate PT government attention on strengthening statutory privacy protections in specific sectors that are exclusively or primarily within PT jurisdiction (e.g., PT public sector organizations²⁴⁷, health organizations [public/private], and PT-regulated employers [private]), at least to the extent that personal information flows between private organizations continue to be intra-PT only and do not become entirely inter-PT or international.
158. Track #1 is the basis for PIAC’s recommendation in the Ontario Privacy Consultation, outlined in detail in Part 4, to: bolster privacy protections in Ontario’s private sector, by GDPR-izing PIPEDA and introducing Ontario employment privacy legislation.

TRACK #2: JOURNEY TOWARD EVENTUAL, NECESSARY & INEVITABLE UNIFIED FEDERAL PUBLIC/PRIVATE SECTOR LEGISLATION

159. Pursuant to Track #2, which is long term (up to 20 years), PIAC **recommends** that FPT governments should plan and take steps on the journey to an eventual – and in PIAC’s view necessary and inevitable – *single federal GDPR-like privacy statute* covering both the private and public sectors. The move to a unified law is required to make Canadian privacy law fully “interoperable” with GDPR and GDPR-ized foreign national privacy laws, especially in light of ongoing digital technology developments (e.g., online data-gathering [through e-commerce and social media], artificial intelligence [“AI”] and algorithmic decision-making, and the “big data” analysis that drives them). As Edward Ryan recognized in 1972: “Privacy is not just an individual interest, but is first and foremost a political value of the highest order. The creation now of a conceptual rubric under which privacy can be protected, both legally as well as ethically, will be as important to the functioning of western democracy at the end of the twentieth century as was the existence of a viable concept of freedom of speech at its beginning.”²⁴⁸
160. We acknowledge that such a move will take considerable time and need to surmount many “hard problems”, including constitutionality questions, which, from a division of powers perspective, centers on GoC’s jurisdiction over the private sector pursuant to PIPEDA, any successor, or a unified federal statute.²⁴⁹ There is little controversy on the ambit of the Privacy Act, or incorporating its provisions into a unified federal statute, since it applies directly to the federal government and its employees.
161. The question of PIPEDA’s constitutional validity focuses on whether the regulation of the commercial collection, use, and disclosure of personal information exceeds the legislative competence conferred on GoC under the *Constitution Act, 1867*, pursuant to its “trade and commerce power” (s. 91[2]) or whether it is *ultra vires* GoC because it legislates in areas of exclusive PT authority, such as “property and civil rights” (s. 92[13], which grants PTs broad jurisdiction over intra-PT trade, and professions and trades within PTs) and health as a local or private matter [s. 92[16]].²⁵⁰

²⁴⁷ This includes PT government institutions, related publicly-funded entities (e.g., municipalities, universities and colleges, public schools, and hospitals [“MUSH sector”]), and their employees.

²⁴⁸ Cited in *Privacy in Canada: A Public Interest Perspective – Address to the Rile Conference on Privacy and Bill C-54*.

²⁴⁹ GoC’s professed power to legislate private sector data protection (in this restricted space) under PIPEDA hinges on the federal trade and commerce power under section 91 ¶2 of the *Constitution Act, 1867*. GoC’s ability to legislate PIPEDA-like data protection in relation to either *interprovincial or international* “data flows” (the so-called “first branch” or “interprovincial or international trade branch”) or to those privacy measures reasonably necessary to other specific heads of power of the Dominion (e.g., telecommunications or banking) generally is not in dispute. What is in dispute is GoC’s ability to legislate PIPEDA-like data protection in relation to *intra-provincial* data flows (the so-called “second branch” or “general trade branch”). While PIPEDA has been generally accepted as constitutionally valid, at least in practice (by individuals and businesses), it has been the subject of constitutional challenge by PT governments (e.g., in 2003, Quebec launched a constitutional challenge against PIPEDA, claiming federal intrusion on PT jurisdiction in relation to property and civil rights under section 92(13) of the *Constitution Act, 1987*; the case has been suspended since 2006).

²⁵⁰ See e.g., *PIPEDA: A Constitutional Analysis*.

162. The debate over PIPEDA’s constitutional validity is currently dormant, however the 2011 SCC case *Reference Re Securities Act*, 2011 SCC 66, [2011] 3 S.C.R. 837 (“Securities Act Reference” or “Securities Reference”) may have placed new limits on the scope of the federal trade and commerce power. In the wake of the decision, former SCC Justice Michel Bastarache suggested “(t)here is a very strong possibility that, in light of the Supreme Court’s decision in the Securities Reference, PIPEDA’s model of cooperative federalism may need to be revised”, noting that “(t)he option for provinces to ‘opt-out’ by enacting substantially similar legislation provides a ‘poor answer’ to the challenge that PIPEDA comprehensively regulates matters which were for the provinces, not Canada, to regulate.”²⁵¹ Bastarache suggests that “it may be necessary to formally recognize provincial legislative jurisdiction over purely intra-provincial aspects of private sector privacy regulation, which extend beyond the national interest in providing minimum standards.” While this has been implicitly assumed (and indeed, justifies the “substantially similar” exemption under PIPEDA), the Bastarache opinion posits that this is no longer good enough. Instead, he suggests, what is needed is real intergovernmental cooperation: “*legally formalized intergovernmental cooperation*” (emphasis added). The shape of such “legally formalized intergovernmental cooperation” is unclear, especially in light of the failure of the Securities Act Reference; however, Bastarache suggests clues lie in the national egg and chicken marketing schemes as possible models.
163. In PIAC’s view, this vision of legally formalized intergovernmental cooperation should be pursued towards a unified federal privacy statute, albeit it would supplant the current “PIPEDA above all” vision based on *General Motors of Canada Ltd v City National Leasing* (“General Motors”) and, thus, would be highly controversial. A formal “intergovernmental governance institution” (“IGGI”), defined as a permanent standing body of intergovernmental officials to negotiate jurisdictional problems, would be essential for GoC and OPCC to make any progress in combining PIPEDA and the Privacy Act with a view to having a more consistent set of privacy statutes that will pass GDPR “adequacy” scrutiny. In any event, PIAC is of the view that private organizations with purely intra-provincial data flows (i.e., that do not flow data to inter-PT and international, especially US, data centres) will be exceedingly rare, in which case PT jurisdiction will be over an increasingly small portion of commerce that is truly internal.
164. Track #2 is beyond the scope of the Ontario privacy consultation, therefore no further details are provided in this submission. However, the constitutionality issue is revisited where relevant.

PART 4: PIAC’S RECOMMENDATION IN THIS CONSULTATION – BOLSTER PRIVACY PROTECTIONS IN ONTARIO’S PRIVATE SECTOR, BY “GDPR-IZING” PIPEDA & INTRODUCING ONTARIO EMPLOYMENT PRIVACY LEGISLATION

165. PIAC **recommends** that privacy protections in Ontario’s private sector should be bolstered, by GDPR-izing PIPEDA and introducing Ontario employment privacy legislation. Each element of this recommendation is detailed separately, below.

RECOMMENDATION #1: BOLSTER PRIVACY PROTECTIONS IN ONTARIO’S PRIVATE SECTOR

Ontario proposal:²⁵² Bridge “gaps” in the Ontario legislative privacy framework, by establishing “comprehensive, up-to-date rules that will protect privacy rights and increase confidence in digital services”.

166. PIAC **recommends** that privacy protections in Ontario’s (and Canada’s) private sector should be strengthened.
167. **Current legislative privacy framework.** As noted, Ontario does not have general private sector privacy legislation. Current Ontario legislation, often described as a “patchwork”, only governs the collection, use,

²⁵¹ The Constitutionality of PIPEDA: A Re-Consideration in the Wake of the Supreme Court of Canada’s Reference re Securities Act (brackets added).

²⁵² Ontario consultation paper, p. 1; Ontario’s Regulatory Registry.

and disclosure of personal information by *public sector* organizations and certain *health sector* organizations (i.e., “health custodians” and their “agents”)²⁵³:

- **Public sector organizations:** *Freedom of Information and Protection of Privacy Act*²⁵⁴ (“FIPPA”) (for provincial institutions such as the Ontario government, select agencies, hospitals, and universities/colleges) and *Municipal Freedom of Information and Protection of Privacy Act*²⁵⁵ (“MFIPPA”) (for municipal institutions, such as municipalities, school boards, transit commissions, and policy service boards); and
- **Health sector organizations:** *Personal Health Information Protection Act*²⁵⁶ (“PHIPA”) (for certain health organizations, such as hospitals, long-term care facilities, and pharmacies).

168. **Gaps in privacy protections.** Due to the absence of Ontario general private sector privacy legislation, PIPEDA applies to private organizations operating in Ontario.²⁵⁷ However, as noted, PIPEDA’s application is limited in scope, creating gaps in legislative privacy protections (“legislative gaps”) for Ontarians, including:

- **Non-commercial organizations & activities:** As noted, PIPEDA – for constitutional division of powers reasons – does not cover *non-commercial organizations* and *non-commercial activities*. Consequently, Ontario non-businesses and intra-Ontario non-commercial activities (of Ontario businesses and non-businesses) are not governed.²⁵⁸
- **Provincially-regulated employees:** As noted, PIPEDA – for constitutional division of powers reasons – only covers employee personal information of FWUBs (which are “a small segment” of Ontario employers)²⁵⁹. Consequently, PIPEDA does not govern the employee personal information of provincially-regulated Ontario private employers (e.g., retail, hospitality, manufacturing, and professional services). Further, since Ontario lacks employment sector privacy legislation, no privacy statute applies to these employers²⁶⁰ (“employee privacy gap”). This said, some privacy protection is provided to employees of provincially-regulated private employers by the *Occupational Health & Safety Act*²⁶¹, common law governs workplace privacy in Ontario (e.g., torts of “intrusion upon seclusion” or invasion of privacy and “public disclosure of private facts”)²⁶², and employers sometimes have their own internal privacy policies, albeit their enforceability depends on many factors.²⁶³

169. In addition to the foregoing legislative gaps, as noted, to the extent that PIPEDA applies in Ontario, PIPEDA’s current privacy rules are outdated, weak, and thus insufficient to successfully address the privacy challenges posed by today’s digital technologies, never mind tomorrow’s.

170. **Establish comprehensive, up-to-date, rules that enhance protection of privacy rights.** Due to the foregoing legislative gaps and flaws, we agree with the Ontario government that “comprehensive, up-to-date rules that will protect privacy rights and increase confidence in digital services” are urgently needed. However, we oppose the Ontario-proposed mechanism to bridge these gaps (i.e., new Ontario general private sector privacy legislation) and disagree with the substance of the proposed Ontario rules.

171. **Prioritize individuals over private organizations.** PIAC is concerned about the Ontario government’s embrace of two *equally prioritized* goals for privacy legislation reform, specifically to equally protect both individual Ontarians and Ontario businesses:

²⁵³ Ontario consultation paper, p. 2; Ontario consultation website.

²⁵⁴ RSO 1990, c F31.

²⁵⁵ RSO 1990, c M56.

²⁵⁶ SO 2004, c 3, which was recently revised via Bill 188, *An Act to enact and amend various statutes*, 1st Sess, 42nd Leg, Ontario, 2020 (assented to 25 March 2020), SO 2020, c 5.

²⁵⁷ See e.g., Ontario consultation news release (“Currently, private sector organizations operating in Ontario must follow the rules set out in the Personal Information Protection and Electronic Documents Act [PIPEDA], which governs traditional commercial activities”).

²⁵⁸ See e.g., COVID-19 Realities Push Ontario Government to Launch Public Consultation to Improve the Province’s Privacy Laws (“[T]here are currently no privacy laws in Ontario that govern non-commercial activities”).

²⁵⁹ Provincial Private Sector Privacy Law Being Considered in Provincial Consultation.

²⁶⁰ See e.g., Blakes: Ontario Government Launches Consultation to Enhance Privacy Protections; Fasken: Privacy and Cybersecurity Bulletin.

²⁶¹ Workplace Privacy, an Increasingly Important Issue in the Information Age.

²⁶² Canada: An Employer’s Guide to Privacy in the Workplace; Privacy Best Practices in a Pandemic Public Health Emergency.

²⁶³ Workplace Privacy, an Increasingly Important Issue in the Information Age.

“In addition to protecting the personal information of individual Ontarians, we also want to ensure that any new privacy protections do not pose unnecessary burden to businesses, or inhibit the growth and prosperity of Ontario’s innovation ecosystem.”²⁶⁴

“We must ensure that digital transformation takes place in a way which enables the benefits of data-driven innovation but minimizes the risks to impacting Ontarians privacy.”²⁶⁵

Together, these statements appear to reflect the stated purpose of PIPEDA:

“to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.”²⁶⁶

172. Instead, PIAC **recommends** that the *primary* purpose of Canadian privacy legislation reform, overall, should be to strengthen protection of the personal information of individual Ontarians and Canadians, specifically to *enhance individuals’ control* over its collection, use, and disclosure (“PIAC foundational belief”). By corollary, PIAC opposes the idea of reducing privacy rules on organizations, both private and public sector. It is crucial to protect Canadians’ privacy rights in an era of “surveillance capitalism” and “government by surveillance”. As OPCC states: “Canadians want to enjoy the benefits of digital technologies, but they want to do it safely. Legislation should recognize and protect their freedom to live and develop independently as persons, away from the watchful eye and unconscious influence of a surveillance state or commercial enterprises, while still participating voluntarily and safely in the day-to-day activities of a modern society.”²⁶⁷
173. The PIAC foundational belief underpins all of our recommendations in this submission, and it is detailed in the PIAC Position Paper on DCTT and Privacy.

RECOMMENDATION #2: DO NOT INTRODUCE ONTARIO GENERAL PRIVATE SECTOR PRIVACY STATUTE; INSTEAD, “GDPR-IZE” PIPEDA & INTRODUCE ONTARIO EMPLOYMENT SECTOR PRIVACY LEGISLATION

Ontario proposal: Strengthen privacy protections in Ontario’s private sector by “creating a unique, made-in-Ontario solution”²⁶⁸, specifically by introducing Ontario private sector privacy legislation of general application.

DO NOT INTRODUCE ONTARIO GENERAL PRIVATE SECTOR PRIVACY LEGISLATION

174. PIAC **opposes** the Ontario government’s commitment to strengthen privacy protections in Ontario’s private sector by “creating a unique, made-in-Ontario solution”²⁶⁹, specifically by introducing Ontario private sector privacy legislation of general application (which, if declared “substantially similar” to PIPEDA would exempt covered entities from PIPEDA with respect to collecting, using, or disclosing personal information *within Ontario*). Key reasons include the following.

REASON #1: NEW ONTARIO GENERAL PRIVATE SECTOR PRIVACY LEGISLATION IS INCONSISTENT WITH PIAC’S POSITION ON CANADIAN PRIVACY LAW REFORM

²⁶⁴ Ontario consultation paper, p. 1; Ontario’s Regulatory Registry.

²⁶⁵ Ontario consultation paper, p. 2.

²⁶⁶ PIPEDA, s. 3.

²⁶⁷ OPCC News release: Commissioner’s Annual Report Sets out Blueprint for How to Modernize Canadian Privacy Laws.

²⁶⁸ Ontario consultation paper, p. 1.

²⁶⁹ Ontario consultation paper, p. 1.

175. New Ontario general private sector privacy legislation would be inconsistent with PIAC’s position on Canadian privacy law reform, outlined in Part 3. Additional details on our position, in the Ontario context, are provided next.

REASON #2: NEW ONTARIO GENERAL PRIVATE SECTOR PRIVACY LEGISLATION WOULD BE ILL-SUITED FOR INCREASINGLY INTER-JURISDICTIONAL PERSONAL INFORMATION FLOWS

176. New Ontario general private sector privacy legislation would not reflect personal information flows, which are increasingly inter-jurisdictional. As we said in 1999: “This problem is not a local issue: it transcends provincial, even national, boundaries. It’s solution must similarly transcend provincial and national boundaries.”²⁷⁰ This is why PIAC proposes designing and implementing a *uniform* modernized (specifically, GDPR-ized) framework that is workable across Canada.

REASON #3: NEW ONTARIO GENERAL PRIVATE SECTOR PRIVACY LEGISLATION WOULD CAUSE MORE PROBLEMS THAN IT SOLVES

177. New Ontario general private sector privacy legislation would cause more problems than it solves, because it could have significant negative impacts on the following.
178. **Canada’s privacy framework.** Canadian privacy protections, which already differ in scope and coverage between and within PTs, would be further fragmented, thereby exacerbating confusion and uncertainty, which could be used by private organizations as an excuse for non-compliance.
179. **PIPEDA & OPCC.** New Ontario rules could be *inconsistent* with PIPEDA (current and revised), which would undermine its effectiveness in the short term and dilute its impact in the long-term. Further, new Ontario rules would *overlap* with PIPEDA, since it would continue to apply to inter-provincial and international commercial activities of Ontario organizations. Consequently, these Ontario organizations would be supervised by multiple privacy commissioners (OPCC and IPC). Finally, an increased role for IPC could result in a reduced and limited role for OPCC.
180. **Ontario businesses & consumers.** New Ontario rules would be a new set of obligations for businesses, requiring new compliance programs (e.g., policies and procedures), resulting in increased compliance costs, which would likely be passed on to consumers, who are already subject to COVID-19 pandemic-related financial pressure. Further, new Ontario rules that are inconsistent with PIPEDA could hamper, rather than “nurture”, innovation.
181. For these reasons, instead of introducing Ontario general private sector privacy legislation, PIAC recommends “GDPR-izing” PIPEDA and introducing Ontario employment sector privacy legislation. These recommendations are examined in turn, next.

“GDPR-IZE” PIPEDA

182. PIAC **recommends** “GDPR-izing” PIPEDA, for the following reasons.

REASON #1: “GDPR-IZING” PIPEDA IS CONSISTENT WITH PIAC’S POSITION ON CANADIAN PRIVACY LAW REFORM

183. “GDPR-izing” PIPEDA would be consistent with PIAC’s position on Canadian privacy law reform, specifically Track #1, outlined in Part 2.

²⁷⁰ Privacy in Canada: A Public Interest Perspective – Address to the Rile Conference on Privacy and Bill C-54.

REASON #2: “GDPR-IZING” PIPEDA IS SUPPORTED BY KEY PRIVACY STAKEHOLDERS

184. Strengthening and specifically, “GDPR-izing”, PIPEDA is broadly supported by key privacy stakeholders (e.g., governments, regulators, businesses, civil society, experts, academics, and individuals). Illustrative examples follow and additional details are provided in Part 4.

185. **GoC support.** Examples of GoC support include:

May 2019 Digital Charter

- Has 10 principles (“Digital Charter principles”), including²⁷¹:
 - **#2 Safety and Security:** “Canadians will be able to rely on the integrity, authenticity and security of the services they use and should feel safe online.”
 - **#3 Control and Consent:** “Canadians will have control over what data they are sharing, who is using their personal data and for what purposes, and know that their privacy is protected.”
 - **#4 Transparency, Portability and Interoperability:** “Canadians will have clear and manageable access to their personal data and should be free to share or transfer it without undue burden.”
 - **#6 A Level Playing Field:** “The Government of Canada will ensure fair competition in the online marketplace to facilitate the growth of Canadian businesses and affirm Canada's leadership on digital and data innovation, while protecting Canadian consumers from market abuses.”
 - **#7 Data and Digital For Good:** “The Government of Canada will ensure the ethical use of data to create value, promote openness and improve the lives of people—at home and around the world.”
 - **#10 Strong Enforcement and Real Accountability:** There will be clear, meaningful penalties for violations of the laws and regulations that support these principles.
- Identifies “programs and initiatives to make Canada a competitive, data-driven digital economy” including “strengthening privacy in the digital age”, which is the focus of the aforementioned GoC Proposals to Modernize PIPEDA (and of “modernizing Canada’s Privacy Act”).²⁷²

May 2019 GoC Proposals to Modernize PIPEDA

- States the Act’s reform “must contribute to the outcomes related to” the Digital Charter principles and emphasizes that: next generation privacy laws in the EU are impacting Canada’s policies and practices; there is “a desire for an approach to personal information protection in the private sector that meets Canada’s needs and remains interoperable with leading jurisdictions”²⁷³; and there are “a number of important distinctions between Canadian and international frameworks” that “are challenging the goal of an integrated digital economy both at the domestic and international levels”.
- States that in modernizing the Act, GoC’s “goal” is to “enhance consumers’ control” (thereby “respect[ing] individuals and their privacy”), “enable responsible innovation” (by private organizations), and “enhance enforcement”. Overall, the proposals include: “clarifications (...) that detail what information individuals should receive when they provide consent; certain exceptions to consent; data mobility; deletion and withdrawal of consent; incentives for certification, codes, standards, and data trusts; enhanced powers for the Office of the Privacy Commissioner; as well certain modernizations to the structure of the law itself and various definitions”.

December 2019 ISED Minister Mandate Letter

- Directs the ISED Minister to work with the Heritage Minister to “create new regulations for companies to better protect people’s personal data and encourage competition in the digital marketplace” (to be overseen by a newly created Data Commissioner).

186. **FPT privacy commissioner support.** FPT privacy commissioners have called for PIPEDA (and Canadian privacy legislation overall) to be strengthened, by aligning it with the laws of other jurisdictions, especially

²⁷¹ Canada’s Digital Charter: Trust in a Digital World.

²⁷² Canada’s Digital Charter: Trust in a Digital World.

²⁷³ Strengthening Privacy in a Digital Age also states: “Interoperability of privacy frameworks is a key foundation of Canada’s approach to privacy”.

the EU. Examples are the October 2019 Joint FPT Privacy Commissioner Resolution (which calls on their respective governments to strengthen Canadian privacy statutes because they have “sadly fallen behind the laws of many other countries in the level of privacy protection provided to citizens”) and OPCC Annual Report 2018-19 (which recommends that “Canadians need stronger (...) federal privacy laws” that “ensure better privacy protection” and notes “several” PT “substantially similar” statutes “offer stronger privacy protections”).

187. **Other privacy stakeholders’ support.** Other privacy stakeholders, including privacy experts, academics, and public interest groups, have criticized PIPEDA for digital privacy and adequacy gaps (albeit there is disagreement on the specific gaps that are identified as requiring change) and called for PIPEDA to be strengthened in response.

REASON #3: JURISDICTIONAL CHALLENGES OF “GDPR-IZING” PIPEDA ARE REAL BUT SURMOUNTABLE

188. Some legal experts contend that certain GDPR elements pose insurmountable constitutional hurdles, because they “cannot be regulated by PIPEDA on account of limitations to federal jurisdiction over ‘trade and commerce’”²⁷⁴, including *non-commercial* organizations and activities and provincially-regulated employers.
189. PIAC believes that making PIPEDA more GDPR-like raises federal-Ontario government jurisdiction issues that are real but surmountable. The issue of provincially-regulated employers can and should be addressed via new Ontario employment sector privacy legislation (see details below). The challenges posed by non-commercial organizations and activities, and other potential areas of primarily or exclusively PT jurisdiction, could ultimately be overcome by adopting the legally formalized intergovernmental cooperation approach to privacy advocated by PIAC in the context of Track #2 of our broader position on Canadian privacy law reform.

INTRODUCE ONTARIO EMPLOYMENT SECTOR PRIVACY LEGISLATION

Ontario proposal: Silent on employee personal information. However, the Ontario consultation paper notes that PIPEDA does not apply to the personal information of most employees and, for this reason, legal experts contend the proposed legislation is intended to cover provincially-regulated employers and employee personal information.²⁷⁵

(Note: Bill 14, the *Personal Information Protection Act*, which died on the Order Paper, “included specific provisions which would regulate the handling of employee personal information by provincially regulated employers in Ontario”²⁷⁶.)

190. PIAC **recommends** that the employee privacy gap should be bridged by introducing Ontario employment sector privacy legislation, for the following reasons.

REASON #1: NEW ONTARIO EMPLOYMENT PRIVACY LEGISLATION IS CONSISTENT WITH PIAC’S POSITION ON CANADIAN PRIVACY LAW REFORM

191. New Ontario employment sector privacy legislation would be consistent with PIAC’s position on Canadian law reform, since Ontario has exclusive jurisdiction over provincially-regulated employers.

²⁷⁴ A New Privacy Law for Ontario?

²⁷⁵ See e.g., Provincial Private Sector Privacy Law Being Considered in Provincial Consultation (“If a provincial privacy law passes, it will likely regulate the employee personal information in all private sector companies in Ontario”); Torys: Ontario Enters the Private Sector Privacy Realm; A New Privacy Law for Ontario?

²⁷⁶ Canada: An Employer’s Guide to Privacy in the Workplace.

REASON #2: WORKPLACE PRIVACY IS INCREASINGLY CONTENTIOUS, HIGHLIGHTED BY COVID-19 PANDEMIC

192. Workplace privacy and employee monitoring are increasingly contentious, highlighted by COVID-19 (e.g., DCTT, including wearables).²⁷⁷ As noted, workplace privacy law pertains to employers and employees, specifically to employers' collection, use, and disclosure of employees' personal information for employment-related purposes. This is a complicated, contentious, and controversial area, due to competing interests: "employees wish to have their privacy rights respected and protected" whereas "employers want to ensure that activity in the workplace does not negatively impact their business".²⁷⁸ Frequently disputed issues include employee medical information and employee monitoring/surveillance (i.e., the extent to which employers may monitor employees within and outside the workplace, such as their Internet use and personal e-mail accounts). For example, OPCC states that it "regularly receive(s) complaints related to workplace surveillance issues – in particular employees raise concerns with respect to video surveillance, which can represent a particularly privacy intrusive collection of personal information".²⁷⁹
193. Employee monitoring, within and outside the *private sector* workplace, is permissible if it complies with: statutory privacy principles; workplace health and safety legislation; labour relations legislation and rulings; particular workplace agreements (collective agreements and arbitrations); and human rights and constitutional law (Charter). Privacy statutes allow for personal data of employees to be collected, used, and disclosed without consent, within the bounds of reasonableness (i.e., for purpose of creating, managing, or ending an employment relationship), provided employers are transparent (i.e., provide notice and reasons, such as employee health-safety).²⁸⁰ In particular:
- "(T)he monitoring must be conducted for a purpose consistent with what a reasonable person would consider appropriate in the circumstances. Canadian privacy regulatory authorities generally use a four-part test to assist in determining the reasonableness of employee monitoring:*
- Is the surveillance demonstrably necessary to meet a specific need?*
 - Is the measure likely to be effective in meeting that need?*
 - Is the loss of privacy proportional to the benefit gained?*
 - Is there a less privacy-invasive way that the employer could achieve the same end?"²⁸¹*
194. In our view, the present situation is untenable. Surveillance, monitoring and potential workplace worker behaviour modification based upon that surveillance and personal information gathering within the workplace represent grave and growing threats to workers' autonomous control of their labour power and any shred of human agency in the workplace. Such a situation is akin to indentured servitude and a form of techno-based deskilling of workers.²⁸²
195. It is PIAC's view that privacy law in the workplace can be an important bulwark against the de-humanization of the worker. Requiring consent to monitor employee activities is not the only benefit of workplace privacy; it also limits the power of the employer over the employee due to inappropriate over-knowledge of personal matters, desires and proclivities of workers via indiscriminate personal data collection (for example, through use of health monitoring apps or devices) that are irrelevant to the employer but that provide potential leverage to unscrupulous employers.
196. We therefore **recommend** that the government of Ontario launch a separate consultation on a provincial employment privacy law to consider these important questions.

²⁷⁷ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 61; Workplace Privacy, an Increasingly Important Issue in the Information Age.

²⁷⁸ Workplace privacy, an increasingly important issue in the Information Age.

²⁷⁹ OPCC Annual Report 2019-20.

²⁸⁰ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 61.

²⁸¹ Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*, p. 61.

²⁸² Labor and Monopoly Capital.

RECOMMENDATION #3: “GDPR-IZE” GENERAL PRIVATE SECTOR PRIVACY LEGISLATION (PIPEDA OR NEW ONTARIO STATUTE) BY ENHANCING ITS SCOPE, PRIVACY PROTECTIONS, & COMPLIANCE/ENFORCEMENT (“PIAC-RECOMMENDED PRIVACY RULES”)

197. PIAC **recommends** that general private sector privacy legislation – PIPEDA, ideally, or a new Ontario statute – should be “GDPR-ized” by enhancing its scope/application, privacy protections (organization obligations and individual rights), compliance, and enforcement (“PIAC-recommended privacy rules”). These recommendations use the current PIPEDA, described in Part 2, as the baseline (i.e., “introduce” a rule means it does not exist in the act) and the current GDPR, also described in Part 2, as the main comparator. Pertinent support for the PIAC-recommended privacy rules by key privacy stakeholders is also identified.

SCOPE/APPLICATION: EXPAND (WITHIN CONSTITUTIONAL LIMITS)

Ontario proposal: As noted, the Ontario government proposes to *expand the scope and application of the law* to include non-commercial organizations (see details below), but is otherwise silent on specifics.

198. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should have expanded scope/application, consistent with constitutional/jurisdictional limits, as follows.

PREAMBLE & PURPOSE STATEMENT: INTRODUCE, TO ENSURE PROPER BALANCE BETWEEN INDIVIDUALS’ RIGHT TO PRIVACY & ORGANIZATIONS’ “LEGITIMATE INTERESTS”

Ontario proposal: Silent.

199. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should include a Preamble and purpose statement that collectively ensure a proper balance between individuals’ right to privacy and organizations’ “legitimate interests”.

200. As noted in the foregoing discussion of PIAC’s foundational belief, current political and policy discourse on Canadian private sector privacy law reform – including the Ontario privacy consultation – evidences a troubling emphasis on (continued) equal prioritization of two objectives: protecting individual privacy and facilitating data-driven business and “innovation”.²⁸³ PIAC believes this equal prioritization reflects and reinforces PIPEDA’s current purpose statement, which effectively “aims to strike a balance between an individual’s right to the privacy of personal information and the need of organizations to collect, use or disclose personal information for legitimate business purposes”.²⁸⁴ However, there is a global policy debate, stated from the business perspective by White & Case LLP, over the “major question (of) where the right balance should lie between the right to privacy and the ability of companies to monetise data about individuals”.²⁸⁵ In PIAC’s view, a new approach is warranted, specifically a “privacy-first” FPT government policy response to public policy issues that *prioritizes* individual privacy.

201. This is why we advocate for general private sector privacy statutes to be rights-based (see details below) and why we recommend inserting corresponding new “Preamble” and “Purpose” statements at the opening of the legislation that, in OPCC’s words²⁸⁶, “entrench privacy in its proper human rights framework” and “also provide the values, principles and objectives to guide how the data protection principles (...) are interpreted and applied” in order to “allow for *responsible innovation that serves the public interest (...)* but

²⁸³ For example, the CMA submission to the BC privacy law consultation seeks “to ensure PIPA remains a flexible law that will enable marketers to serve consumers effectively while protecting their privacy interests”: Privacy Update – Provincial Privacy Law Reform, Final CCPA Regulations and More.

²⁸⁴ Canada’s Federal Privacy Laws: Background Paper.

²⁸⁵ Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018* (bracket added).

²⁸⁶ OPCC Annual Report 2019-20 (emphasis added).

prohibit using technology in ways that are *incompatible with our rights and values*". In particular, the legislative purpose should be, in OPCC's words:²⁸⁷

- **Purpose #1:** to implement "the fundamental right to privacy (...) in the commercial context through robust data protection that ensures that the processing of data is lawful, fair, proportional, transparent and accountable, and respects the fundamental rights and freedoms of individuals".
- **Purpose #2:** to "balance privacy rights" against *other rights*, "a legitimate *public interest*", and "the *legitimate interest of organizations* to collect, use and disclose personal information for purposes that a *reasonable person would consider* appropriate in the circumstances and in ways that *do not represent surveillance*". Further, PIAC suggests statutory clarification that "reasonable person" means a reasonable individual (not organization).
- **Purpose #3:** to "provide individuals with quick and effective remedies when their privacy rights have not been respected and to ensure the ongoing compliance by organizations with their (statutory) obligations".

202. This language would help to ensure "that individuals are not viewed as a commodity...privacy is not a right we simply trade away for innovation, efficiency or commercial gain".²⁸⁸

"PERSONAL INFORMATION": CLARIFY & EXPAND

Ontario proposal: Silent.

203. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should clarify and expand the definition of "personal information", within constitutional division of powers limits, in ways including the following.
204. **Include identifiers within definition of "personal information"**. PIAC **recommends** that the definition of "personal information" should include identifiers and, at minimum, these should reflect the identifiers in the GDPR definition of personal data detailed in Part 2.
205. **Define "sensitive personal information"**. PIAC **recommends** that legislation should define "sensitive personal information" to, at minimum, reflect the GDPR definition of personal data detailed in Part 2.
206. **Define "de-identified information"**. PIAC **recommends** that legislation should define "de-identified information" (and its variants – see details below), including specifying that de-identified information is only "non-personal information" (hence, excluded from certain elements of the statute) – if it can be proven *beyond a reasonable doubt* (not "reasonable possibility" or "serious possibility") that it can never be re-identified. The definition should be accompanied by a framework for the use of de-identified data *with consent*, meaning consent is required to de-identify data, and to subsequently collect, use, and disclose the resulting de-identified data, unless strict conditions are met.

²⁸⁷ OPCC Annual Report 2019-20 (emphasis and bracket added).

²⁸⁸ OPCC Annual Report 2019-20.

NON-COMMERCIAL ORGANIZATIONS & ACTIVITIES: INCLUDE (WITHIN CONSTITUTIONAL LIMITS)

Ontario proposal: As noted, the Ontario government proposes to *expand the scope and application of the law* to include “non-commercial organizations, including not-for-profits, charities, trade unions and political parties”.²⁸⁹ The proposal is silent on non-commercial activities. However, the Ontario consultation paper notes that PIPEDA does not apply to non-commercial activities and, for this reason, certain legal experts contend the Ontario government “may be contemplating” expanding the law to non-commercial activities.²⁹⁰

207. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should expand covered entities to *non-commercial* organizations – including but not limited to not-for-profits, charities, professional associations, trade unions, and political parties – and *non-commercial* activities (of businesses and non-businesses). We agree with the Ontario consultation paper²⁹¹ that it is important for all personal information to be “consistently protected”, regardless of whether it is held by a business or non-business. However, we believe that political parties could be better covered under public sector privacy statutes (Privacy Act [federal parties] or Ontario [provincial parties]).²⁹²
208. This PIAC recommendation is supported by certain key stakeholders, including GoC and Canadian privacy commissioners. For example, the October 2019 Joint Resolution by FPT Privacy Commissioners calls for all private (and public) sector entities engaged in handling personal information to be subject to privacy laws. GoC’s Proposals to Modernize PIPEDA include considering extending its application to “non-commercial data collection activities”, in order to recognize that “(a) growing number of organizations and entities are engaging in (them)” and “to ensure that Canadians are protected and businesses have a level playing field and that accountabilities – along with the responsibilities that entails – are appropriately apportioned”.²⁹³
209. Expansion of legislation to non-commercial organizations would also align with the current general private sector privacy legislation of Alberta, British Columbia, and Quebec²⁹⁴, and with Quebec Bill 64, which applies to political parties.²⁹⁵
210. We acknowledge that implementing the PIAC recommendation *in PIPEDA* could pose a constitutional challenge in terms of GoC’s jurisdiction being limited to commercial organizations/activities. However, PIAC believes this challenge could be overcome via the legally formalized intergovernmental cooperation approach to privacy advocated by PIAC in the context of Track #2 of our broader position on Canadian privacy law reform.

EXTRATERRITORIALITY: CLARIFY

Ontario proposal: Silent.

211. PIAC **recommends** that general private sector privacy legislation (PIPEDA or Ontario) should clarify extraterritoriality (i.e., application to transborder data flows).²⁹⁶ For details, see discussion below on data transfers to other countries.

²⁸⁹ Ontario consultation release, p. 3; Ontario consultation paper, p. 3.

²⁹⁰ Torys: Ontario Enters the Private Sector Privacy Realm.

²⁹¹ Ontario consultation paper, p. 7 (bracket added).

²⁹² Regarding federal political parties, the *Elections Modernization Act* requires political parties to create and publish a privacy policy. OPCC Annual Report 2018-19 notes: “Joint OPCC-Chief Electoral Officer Guidance for federal political parties on protecting personal information, issued in April 2019, ‘help(s) political parties comply with their new legal obligations relating to privacy policies, but it also outlines a number of privacy best practices’”.

²⁹³ GoC’s Proposals to Modernize PIPEDA.

²⁹⁴ Ontario consultation paper, p. 7.

²⁹⁵ Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

²⁹⁶ See also *Lawson v. Accusearch*, 2007 FC 125. Online: <https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/53507/index.do>

212. This recommendation is supported by certain key stakeholders, including GoC. For example, GoC's Proposals to Modernize PIPEDA include "updating and clarifying" the "applicability of the Act (...) including in the context of transborder data flows".

PERIODIC REVIEWS: MAINTAIN

Ontario proposal: Silent.

213. PIAC **recommends** that general private sector privacy legislation (PIPEDA or Ontario) should maintain mandated periodic reviews, every 5 years (as per the current federal act), if not earlier, to keep pace with the rapidly evolving digital technology marketplace and its corresponding privacy impacts on individuals.

PRIVACY PROTECTIONS (OVERALL): CLARIFY & ENHANCE

Ontario proposal: As noted, the Ontario government proposes to strengthen privacy protections. Specifically, it seeks to clarify and enhance *specified* privacy protections, both privacy principles/organization obligations and individual rights.

214. PIAC **recommends** that general private sector privacy legislation (PIPEDA or Ontario) should clarify and enhance privacy protections (overall), as follows.

SUBSTANCE: CLARIFY, CAST IN LEGAL LANGUAGE & CONTEMPLATE PRIVATE-PUBLIC PARTNERSHIPS

Ontario proposal: Silent.

215. **Clarify and cast in legal language.** PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should clarify and cast in legal language privacy protections (i.e., move to enforceable rules from unenforceable principles or, put differently, codify principles in declarative language in the text of the act), modeled on declarative statutes like PIPA AB. This would enhance the ability of private organizations to understand their obligations and the ability of individuals to determine and challenge organizations' (non-) compliance, and recognise that results unfavourable to individuals are to be expected, and have been experienced, in standards-based, non-prescriptive Canadian privacy legislation.
216. This PIAC recommendation is supported by certain key stakeholders, including GoC and OPCC. For example, GoC's Proposals to Modernize PIPEDA include clarifying *all* privacy rules, specifically redrafting them "to set out personal information protections, rights and requirements in a manner that is easier for all to understand". The reason is that PIPEDA is hard for individuals, organizations, and courts to comprehend, due to "(h)aving rights and obligations contained in Schedule 1, instead of in the body of the law, and cast in non-legal language, mixing obligations with best practices (shall v. should)".²⁹⁷ OPCC Annual Reports 2018-19 and 2019-20 assert that courts have noted PIPEDA's "non-legal drafting" makes the act inaccessible to the public and covered entities and gives little, if any, guidance to those who must interpret it. Thus, these Annual Reports propose the revised PIPEDA should: "(d)raft the law in the usual manner of legislation, conferring rights and imposing obligations"; "set explicit limits on permissible uses of data, rather than (...) rely on the good will of companies to act responsibly"; "put an end to self-regulation, meaning in part that it should no longer be drafted as an industry code of conduct", and make "(r)espect for privacy rights" a

²⁹⁷ GoC's Proposals to Modernize PIPEDA (explaining that GoC incorporated the CSA Model Code – developed by industry, consumer groups, academics, and government – into the Act "without changes to the language" because it thought "this would be the most effective and expeditious way to act in a very short timeframe").

“clearly codified and enforceable requirement” rather than “a suggested best practice left to the goodwill of (...) big tech”.

217. **Address private-public partnerships.** Further, PIAC **recommends** that legislation should properly contemplate privacy protections in the context of public-private partnerships.
218. This PIAC recommendation is supported by certain key stakeholders, including OPCC. For example, OPCC Annual Report 2019-20 stresses that, even prior to the COVID-19 pandemic, increased reliance on public-private partnerships “had reached a tipping point where privacy and democratic rights were strained and reform was overdue” because “the law has not properly contemplated privacy protection in the context of public-private partnerships”, and highlights the “lack of clarity around data collected for a public purpose by a private entity”, which “could potentially result in a company releasing an application and using the information for commercial purposes, provided consent is obtained, even if it is done in incomprehensible terms”.

SCALABILITY: CONSIDER INTRODUCING, FOR NON-COMMERCIAL ORGANIZATIONS ONLY (ESPECIALLY NFPs & CHARITIES)

Ontario proposal: Silent. However, the Ontario government proposes scalable *compliance* (see details below).

219. PIAC **recommends** that if the scope of general private sector privacy statutes (PIPEDA or Ontario) is expanded to non-businesses, then scalability of privacy protections— in terms of proportionality standards, different rules, and/or different thresholds based on size and status – should be considered, especially for NFPs and charities. A one-size-fits-all legislative approach to non-businesses might not be appropriate.
220. For clarity, PIAC **opposes** scaled privacy protections for businesses, based on specified thresholds (e.g., size, such as SMEs), whether by excluding certain business categories from obligations or changing the way that obligations are implemented (e.g., by making certain obligations “lighter”). In the context of rapidly advancing surveillance technology available to businesses (and governments), the highest possible standard for all should be imposed, with minimal carve-outs creating categories of organizations that are subject to different (particularly, lessened) privacy rules. This extends to the “data controller” versus “data processor” distinction in GDPR.
221. However, if scalable privacy protections for businesses is introduced, then PIAC **recommends** strict definitions of relevant business categories, taking into consideration how businesses could try to manipulate their designations and practices to “pass off” personal information to subsidiaries or third parties that are subject to lesser requirements. This risk could be mitigated by a statutory provision prohibiting organizations from escaping their privacy obligations through sub-contracting or blaming third-party violations.
222. For our separate position on scalability of *enforcement*, see below.

ORGANIZATION OBLIGATIONS: ENHANCE

Ontario proposal: As noted, the Ontario government proposes to clarify and enhance *specified* privacy principles/ organization obligations.

223. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should strengthen organization obligations, as follows.

PRIVACY BY DESIGN (“PbD”): INTRODUCE

Ontario proposal: Silent.

224. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should require PbD, even if, as some businesses suggest, it is already recognized as best practice. Mandated PbD “build(s) privacy assurance into the very design of a product, service or initiative, from the early phase of conception through to its execution, deployment and beyond” and implements *demonstrable* accountability.²⁹⁸ The proviso is that PbD must be accompanied by other elements of demonstrable accountability, including mandated PIAs, as detailed below.
225. This PIAC recommendation is supported by certain key stakeholders, including Canadian privacy commissioners. For example, OPCC Annual Report 2018-19 proposes mandating PbD, as one element of demonstrable accountability.
226. Mandating PbD would also align with existing and proposed legislative regimes, both international and Canadian. For example, PbD is mandated in various European jurisdictions, pursuant to GDPR (where its implementation is ensured through mandated DPIAs) and numerous non-EU jurisdictions.²⁹⁹ Quebec’s Bill 64 also mandates PbD, albeit only for organizations “offering a technological product or service”, and it is uncertain what organizations would count: “This could be a narrow requirement (e.g., manufacturers of devices that collect personal information, such as mobile phones) or it could be much broader (e.g., enterprises which offer service online and use any kind of online metrics).”³⁰⁰
227. Further, PIAC **recommends** the allocation of government funding for PbD initiatives.

TRANSPARENCY: INCREASE

Ontario proposal: As noted, the Ontario government proposes to *increase transparency*, by providing individuals with more detail about how their information is being used by businesses and non-businesses.³⁰¹ According to the Ontario consultation paper³⁰², organizations are required to publish details about their privacy practices (i.e., collection, use, and disclosure of personal information), “in service policies and privacy statements”, but individuals are unlikely to engage with it because it is written in dense legal jargon. For this reason, “alternative models” that better inform Ontarians are being considered, including requiring organizations to use “clear and plain language” to state “what personal information is collected, how it is collected, how it is used, and with which third parties (it) will be shared”.

228. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should increase transparency, because it is required for meaningful consent. Consideration also should be given to requiring information structuring tools such as “privacy boxes” in certain online contexts, to assist consumers in making meaningful consent decisions in those environments.³⁰³
229. This PIAC recommendation for general increased transparency is supported by certain key stakeholders, including Canadian privacy commissioners. For example, the October 2019 Joint Resolution by FPT Privacy Commissioners calls for “transparency requirements to the public” to be “strengthened with respect to the privacy practices of (...) private entities, including information sharing initiatives”.

²⁹⁸ OPCC Annual Report 2018-19.

²⁹⁹ OPCC Annual Report 2018-19.

³⁰⁰ Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR.

³⁰¹ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

³⁰² Ontario consultation document, p. 4.

³⁰³ See A. Lau, “The Privacy Box: Enabling Consumer Choice and Meaningful Consent in Online Privacy” (Ottawa: PIAC, June 2017). Online: <https://www.piac.ca/wp-content/uploads/2017/08/PIAC-THE-PRIVACY-BOX-OCA-REPORT-June-2017-ENG-FINAL.pdf>

230. In particular, PIAC **recommends** that transparency should be increased by requiring organizations to use clear and plain language to state what personal information is collected, how it is collected, how it is used, and with which third parties it will be shared. Transparency should be further enhanced to reflect GoC's Proposals to Modernize PIPEDA, by:
- **Language:** Requiring "specific, standardized" plain-language.
 - **Unbundling:** Prohibiting the bundling of consent into a contract.
 - **Automated decision-making:** Requiring organizations to provide information about the use of automated decision-making ("algorithmic transparency"), specifically: its use; factors involved in the decision and, where the decision is "impactful", information on "the logic upon which the decision is based", to recognize "the misuse of personal information that can result in undue discrimination and bias".
 - **Accountability:** Requiring organizations to "demonstrate their accountability, including in the context of transborder data flows" ("demonstrable accountability").
231. The PIAC recommendation on algorithmic transparency is supported by additional key stakeholders, such as Canadian privacy commissioners. For example, the October 2019 Joint Resolution by FPT Privacy Commissioners calls for a legislative framework to ensure responsible development and use of AI and machine-learning ("ML") technologies. Algorithmic transparency also aligns with proposed Canadian legislative regimes, such as Quebec Bill 64's rights in relation to profiling.

CONSENT: ENHANCE & MINIMIZE EXCEPTIONS/ALTERNATIVE BASES

Ontario proposal: As noted, the Ontario government proposes to *enhance consent* provisions, by "allowing individuals to revoke consent at any time" and adopting "an 'opt-in' model for secondary uses of their information".³⁰⁴ According to the Ontario consultation paper³⁰⁵, additional "alternative models" are being considered, including:

- "(C)larifying consent requirements", which "would include clarifying exceptions to consent", defined as "instances where individual consent is *not necessary, practicable or appropriate*, such as in instances where the collected data has been 'de-identified' or 'derived'... and used to benefit the individual or the overall public good (e.g. for purposes of research or innovation)" (emphasis added).

(Note: Regarding "exceptions to consent", some legal experts correctly note it is uncertain whether and to what degree the Ontario government is considering "free-standing bases on which to process personal information other than consent".³⁰⁶ For this reason, PIAC refers to "exceptions and/or alternative bases".)

- *Where there is no exception*, requiring organizations to "obtain affirmative, demonstrable, informed, and unambiguous consent" (also described as "requiring individuals to 'opt-in' to the collection, use, or disclosure" and requiring opt-in as "the default setting").

(Note: This proposal appears to be inconsistent with a separate statement that confirms the opt-in model is *for secondary uses only*: "Through clear transparency requirements, individuals would understand when and how their personal information is collected, and *only be required to consent for collections, uses, and disclosures of personal information that are outside the organization's described practices*" [emphasis added]).

232. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance consent and minimize exceptions and/or alternative bases to consent, as follows. First, however, we believe it is important to distinguish between critical elements of "consent" that are ignored or glossed over in the Ontario proposal, including: the need for consent; and the nature of "valid" consent, which includes but is not limited to "informed/meaningful" consent (with criteria for making this determination, including those outlined above under transparency) and methods of obtaining consent.

³⁰⁴ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

³⁰⁵ Ontario consultation document, pp. 4-5.

³⁰⁶ See e.g., A New Privacy Law for Ontario?

CONSENT: ENHANCE

233. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance consent, by providing more meaningful control to individuals over their personal information. We believe that consent continues to be the right legal basis for a general privacy standard in Canada. In particular, consent should be enhanced in ways that include the following.
234. **Define, and specify required information, for “informed” consent.** PIAC **recommends** that legislation should define “informed” consent and, consistent with GoC’s Proposals to Modernize PIPEDA, specify what information is needed as the basis for meaningful consent³⁰⁷ (e.g., what and how information must be communicated to the individual at the time of collection, and for new uses). The start point should be the May 2018 joint OPCC, AB and BC Privacy Commissioners’ “Guidelines for Obtaining Meaningful Consent”, which “increased the requirements set out in (their) office’s guidelines for obtaining consent”³⁰⁸ pursuant to PIPEDA and “similarly situated” PT general private sector privacy legislation, which include:
- **Better descriptions:** more accessible and digestible descriptions of the information collected (e.g., for what purposes it will be collected, used and disclosed, with whom it is being shared, and what uses are not essential for service provision) and notification of meaningful risks of harm in using the service.
 - **More control:** enable individuals to control the level and timing of detail.
 - **Improved consent processes:** design and/or adopt innovative processes that can be implemented “just in time”, are context-specific, and interface-appropriate.
235. **Specify types of consent and notice standards.** PIAC **recommends** that legislation should specify the types of consent and their definitions, and clarify that there are at least three different kinds:
- **Express/explicit:** defined by PIAC as situations where the individual expressly provides consent³⁰⁹ (e.g., via “positive option” or “opt-in” [say “yes”]).
 - **Implied/implicit:** defined by PIAC as situations where the individual would have consented if asked, and where the *facts* clearly suggest that consent was provided.³¹⁰
 - **Deemed:** defined by PIAC as situations where it cannot reasonably be determined that the person would have consented if asked, and the *law* permits organizations to act as if the individual has consented (e.g., via “negative option” or “opt-out” [say “no”], but other forms exist).
- Different standards of notice should be applied as appropriate and, additionally, negative option consent should be made subject to criteria for validity.
236. **Set default type of consent (express).** PIAC **recommends** that legislation should set the default type of consent, and we support Ontario’s proposal that organizations generally should be required to obtain *express* consent, specifically to “obtain affirmative, demonstrable, informed, and unambiguous consent” (also described as “requiring individuals to ‘opt-in’ to the collection, use, or disclosure” and requiring opt-in as “the default setting”). Organizations should also be required to keep a record of said express consent, for as long as the personal information is retained and for a reasonable period after its destruction.
237. This PIAC recommendation would align with existing international legislative regimes (e.g., GDPR) and proposed Canadian legislative regimes, specifically Quebec Bill 64, which requires that consent be “clear, free and informed”, given for each separate purpose (which must be requested in “clear and simple language and separately from any other information provided”), and remain valid only for the time needed

³⁰⁷ GoC’s Proposals to Modernize PIPEDA include enhancing consent by specifying what information is needed as the basis for meaningful consent (e.g., the GoC-proposed transparency requirement detailed above).

³⁰⁸ September 2020 OPCC Appearance on Quebec’s Bill 64 (bracket added).

³⁰⁹ See e.g., Did the Supreme Court of Canada formally establish a new form of consent? (defining express consent as “where the individual has expressed his or her consent at the time”).

³¹⁰ See e.g., Did the Supreme Court of Canada formally establish a new form of consent? (defining implied consent as “consent where you can imply someone’s permission or consent from the circumstances”).

to achieve the purpose, following which the personal data must be destroyed or anonymized.³¹¹ Bill 64 also requires organizations to help the individual understand the terms and implications of the consent.³¹² “Sensitive” information, defined as entailing a high level of reasonable expectation of privacy due to its nature or context, would also require express consent.³¹³

238. **Prohibit incompatible secondary processing.** PIAC **recommends** that legislation should prohibit any secondary processing of personal information that is incompatible with the original purpose of collection.
239. **Require opt-in consent for secondary purposes.** PIAC **recommends** that legislation should require opt-in consent for collecting, using, or disclosing personal information for secondary purposes.
240. **In particular, require consent for de-identification.** PIAC **recommends** that consent should be required for “de-identification”, used here as an umbrella term for the spectrum of de-identification (e.g., pseudonymization to true anonymization) that is detailed in the next section. Put differently, the processing of personal information in order to de-identify it (i.e., the act of de-identification) is a secondary “use” that prima facie is not compatible with the original purpose for which it was initially collected and therefore requires (express) consent. This alleged “barrier” to unfettered commerce could be easily addressed by organizations informing individuals at the time of initial collection that their data will be de-identified, and to what degree. We concede that once personal data is *truly anonymized* – which in practice is nearly impossible to achieve – it is no longer personal data, thus subsequent/secondary uses would no longer be regulated, thus the act of *truly anonymizing* personal data does not require consent. This position is supported by Opinion 05/2014 of the Article 29 Working Party on Anonymisation Techniques, which states that, under GDPR, the processing of personal data to *truly anonymize* it is “compatible with the original purposes of the processing” and therefore does not require an additional legal basis (consent or otherwise).³¹⁴
241. **Limit warrantless surveillance.** PIAC **recommends** that legislation should limit the scope of warrantless surveillance and personal information collection by law enforcement.
242. **Require PbD.** As noted, PIAC **recommends** that legislation should adopt PBD as a requirement, provided it is accompanied by enhanced accountability, specifically demonstrable accountability, including mandated PIAs (see details below).
243. **Back-stop with technological tools.** PIAC **recommends** that, ultimately, the requirement to obtain informed consent should be backstopped by privacy-enhancing technologies and tools (e.g., simple and standardized privacy settings, trustmark systems overseen by privacy commissioners, and data tags which would erase data at a particular time).
244. **Require consent except for specific, legislated circumstances.** PIAC **recommends**, consistent with the October 2019 Joint Resolution by FPT Privacy Commissioners, that individuals should “have control over their personal information including real choice and meaningful consent, *except for specific circumstances included in privacy legislation*” (emphasis added). This position is elaborated next.

EXCEPTIONS/ALTERNATIVE BASES TO CONSENT: MINIMIZE NUMBER & PERMIT ONLY WHERE CONSENT NOT “REASONABLY PRACTICABLE” & FOR NARROW RANGE OF “PRESCRIBED PURPOSES”

245. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should:
 - *minimize* the number of exceptions to consent (which we support) or alternative bases to consent (which we oppose);
 - *permit* exceptions only where consent is not *reasonably practicable* (to ensure privacy continues to be respected in these situations) and for a *narrow range of prescribed purposes* (i.e., acceptable practices

³¹¹ Quebec to Introduce the Most Punitive Privacy Laws in Canada; Torys: Ontario Enters the Private Sector Privacy Realm.

³¹² Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR.

³¹³ Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR; Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

³¹⁴ Does Anonymization or De-identification Require Consent under the GDPR? (citing Opinion 05/2014).

for which personal information can be collected, used, or disclosed without consent) – noting that what constitutes “prescribed purposes” is likely to be a highly contested topic; and

- *ensure* exceptions are accompanied by *demonstrable* accountability.

Each of these elements merits further elaboration.

246. **Permit statutory exceptions (but not alternative bases) to consent.** PIAC **recommends** that certain statutory *exceptions to consent* should be identified, to facilitate collection, use, and disclosure of personal information without consent by private organizations (and governments). We agree with OPCC’s recent statement³¹⁵ that “it is essential to state that in 2020, privacy protection cannot hinge on consent alone” because “the power dynamic is too uneven” making it “neither realistic nor reasonable to ask individuals to consent to all possible uses of their data in today’s complex information economy”. On one hand, “consent can be used to legitimize uses that, objectively, are completely unreasonable and contrary to our rights and values”, whereas on the other hand, “refusal to provide consent can sometimes be a disservice to the public interest”. For clarity, PIAC **opposes** any potential shift from a consent-based regime with exceptions to a regime where consent is one of many *alternative bases* for legal processing of personal information (e.g., GDPR model). We note that OPCC, in Annual Report 2018-19, proposes including statutory “exceptions to consent” or “alternative solutions (to meaningful consent)” and, in its September 2020 appearance on Quebec’s Bill 64, refers to “the European approach/model” as “one example” that “merits consideration, among others”.³¹⁶
247. **Minimize number of exceptions/alternative bases to consent, and permit only for specific, legislated circumstances.** PIAC **recommends** that the number of statutory exceptions to consent (which we support) or alternative bases to consent (which we oppose) (i.e., “unconsented collection, use, and disclosure”) should be minimized and permitted only for specific, legislated circumstances, in particular:
- where consent is not *reasonably practicable* (clarifying that “reasonableness” should be in the eyes of the individual), to ensure privacy continues to be respected in these situations; and
 - for a *narrow range of prescribed purposes*. By corollary, we oppose Ontario’s proposal that exceptions should be permitted in all “instances where individual consent is not necessary, practicable or appropriate”, which is a subjective and overly broad test that is open to abuse by organizations, especially those with a profit motive to maximize their collection, use, and disclosure of personal information.
248. **Identify appropriate exceptions to consent (aka “appropriate prescribed purposes”, “appropriate specific circumstances”, or “acceptable practices for unconsented collection, use, and disclosure”).** Identifying the full range of appropriate exceptions to consent is beyond the scope of this submission. In principle, PIAC agrees with OPCC’s recommendation, in its September 2020 appearance on Quebec’s Bill 64, that exceptions to consent should only be permitted “in the public interest, in the pursuit of legitimate purposes or for the common good, within a rights-based regime” that “require(s) businesses and government departments to be transparent and to demonstrate accountability to the regulating authority”.³¹⁷ Otherwise, we restrict our comments in this submission to the Ontario-proposed exceptions to consent, which appear to be:
- “collections, uses, and disclosures of personal information that are (within) the organization’s described practices” (bracket added) (“standard business practices”);
 - de-identified and derived data; and
 - data trusts.

³¹⁵ September 2020 OPCC Appearance on Quebec’s Bill 64.

³¹⁶ OPCC Annual Report 2018-19; September 2020 OPCC Appearance on Quebec’s Bill 64, describing the model as (bracket added): “data can be used (without consent) when it is necessary for the performance of a task carried out in the public interest or for the purpose of the legitimate interests pursued by a business or public entity, while respecting basic rights”.

³¹⁷ September 2020 OPCC Appearance on Quebec’s Bill 64.

We note these Ontario-proposed exceptions to consent are consistent with GoC’s Proposals to Modernize PIPEDA by identifying “certain alternatives or exceptions to consent to facilitate use of personal information by business under specific circumstances”, such as “common uses of personal information for standard business activities” and use/disclosure of de-identified information.

“STANDARD BUSINESS PRACTICES”: DO NOT INTRODUCE EXCEPTION

Ontario proposal: As noted, the Ontario government proposes a new exception to consent for standard business practices.

249. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should **not** introduce a “standard business practices” exception to consent, because this could be interpreted too liberally, permitting all manner of (illegitimate) uses.
250. This PIAC recommendation is supported by certain key stakeholders, including Canadian privacy commissioners. For example, OPCC Annual Report 2019-20 expresses “concern” the standard business practices exception is “much too broad of a concept, one that risks becoming a catch-all exception, if not a gaping hole” and “(b)usinesses should not be allowed to dispense with consent merely because a practice is one they determine to be ‘standard’”.
251. A standard business practices exception to consent would also be mis-aligned with GDPR, specifically with “legitimate interests” as a lawful basis for processing, because in the words of OPCC: “In order to rely on the legitimate interest provision, an organization must first explain the purpose and demonstrate the necessity of the processing, and further justify that the organization’s interests do not infringe upon individuals’ interests, rights or freedoms. Moreover, organizations relying on legitimate interests are required to consider individual objections.”³¹⁸

DE-IDENTIFIED & DERIVED DATA: INTRODUCE RESTRICTIONS & PERMITTED USES

Ontario proposal: As noted, the Ontario government proposes to introduce requirements for, and opportunities to use (aka “restrictions and permitted uses for”), data that has been de-identified and derived from personal information, to provide clarity of applicability of privacy protections.³¹⁹ According to the Ontario consultation paper³²⁰, de-identified data (defined as information pooled in a way that prevents “identification of any individuals’ personal data”³²¹) and derived data (defined as information not directly supplied by customers, such as assessments/evaluations and web-browsing habits) “does not fit neatly into” the Canadian privacy framework. For this reason, a clear set of rules on de-identified and derived data would be created, including “defining these concepts more clearly in law”. Further, since de-identified data “reduces the risk of privacy breaches”, organizations would be encouraged to develop/improve de-identification practices (e.g., via incentives to design “privacy protective applications” and create “new technical standards”).

252. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce clear statutory definitions and rules – both restrictions and permitted uses – for “de-identified information” and “derived information”. We believe that de-identifying and deriving data could be *privacy-protecting* (not “privacy-enhancing”³²²) methods, if done effectively and in appropriate contexts. Our position on de-identified data is elaborated next and should be read together with our separate recommendations on data trusts.

³¹⁸ OPCC Annual Report 2018-19.

³¹⁹ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

³²⁰ Ontario consultation paper, p. 8.

³²¹ Methods of de-identification include removing “identifiers” (e.g., names, identifying numbers), obscuring information (e.g., giving age range in place of exact age), and removing or aggregating information about outliers or small cell size data subjects (e.g., where fewer than 5 people have same postal code): Ontario consultation paper, p. 8.

³²² See e.g., Canadian Anonymization Network FAQ.

253. **Statutorily define “de-identified information”.** As noted, PIAC **recommends** that “de-identified information” and related terms, such as “anonymized information”, “pseudonymized information”, “aggregate information”, and “publicly available information”³²³ should be statutorily defined. Statutory definitions are critically important, to provide a standard lexicon that is shared by all stakeholders, including organizations-individuals (for privacy policies and practices), organizations-organizations (for service agreements) and organizations-regulators (for demonstrating/determining accountability/compliance), and would be consistent with GoC’s Proposals to Modernize PIPEDA, which include adding a statutory definition of “de-identified information” and “exploring” the definition of “publicly available information”.
254. At this time, PIAC does not have a position on the proper definitions of the foregoing terms. However, we note that Quebec Bill 64 defines “de-identified” information as information that no longer directly identifies an individual and “anonymous” information as information that “irreversibly no longer allows the person to be identified directly or indirectly”.³²⁴
255. **Consistently define de-identified information.** PIAC **recommends** that the foregoing terms should be defined in a way that is consistent or at least interoperable with the definitions of other jurisdictions, particularly GDPR.
256. **Contextually define de-identified information.** PIAC **recommends** that statutory definitions should take what CANON calls a “spectrum approach to de-identification”, defined as “the adoption of a spectrum of identifiability” – ranging from identifiable, to various degrees of risk of being re-identified (e.g., “pseudonymized”), to zero risk of being de-identified (e.g., “truly de-identified” or “truly anonymized”) – to replace “the existing black or white approach in which information is either identifiable or non-identifiable – completely in or out of (the privacy statute’s) ambit – respectively”.³²⁵ This approach would acknowledge the reality that, as noted in Part 2, “the binary concept of personal information is no longer fit for purpose” (i.e., there is no bright line between “personal information” and “non-personal information”) because “complete anonymization for which there is virtually no risk of identifying an individual is becoming practically unattainable” (i.e., truly “de-identified information” does not exist) and “de-identification is a relative concept that requires a contextual evaluation”³²⁶ and “definitions (that) allow for consideration of contextual factors” (e.g., nature of data involved; reasonable expectations of potentially affected individual(s); intended purposes for its use; release environment; availability of other linkable data; likely incentives to re-identify data; costs and level of expertise required to re-identify data; and potential harm to individuals should an individual be re-identified).³²⁷ We believe this approach would clarify that all personal information that is not “truly de-identified” (i.e., zero risk) still retains a privacy interest and thus is within the scope of privacy legislation and must be protected.
257. **Do not “flexibly” define de-identified information.** PIAC notes CANON’s identification of two potential *approaches* to the definition of de-identified data (whatever definition is chosen) – “setting out highly specific criteria or prescriptive processes for how personal information is to be de-identified” versus “focusing on the end state that must be achieved” – and its endorsement of the latter for its “flexibility”, to “avoid the risk of constraining innovation (or potentially lessening privacy protections) with definitions which at some point in the near future may become no longer relevant or fit for purpose”.³²⁸ We disagree. Our preliminary position is that a statutory framework for de-identification would be preferable for its certainty and clarity, which benefits individuals, and could be achieved by incorporating existing Canadian privacy commissioner guidance, such as IPC’s “De-Identification Guidelines for Structured Data”³²⁹, which

³²³ “Publicly available” information is defined in PIPEDA Regulations as information appearing in telephone directories, professional or business directories, government registry information, and records of quasi-judicial bodies that are available to the public and “(g)enerally speaking, no consent is required as long as the collection, use and disclosure of such information relates directly to the purposes for which it was made publicly available”: OPCC: FAQ for Online Consent.

³²⁴ Quebec Bill 64, ss. 102 and 111. See also: Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business.

³²⁵ Canadian Anonymization Network: Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’ (bracket added, replacing “PIPEDA”).

³²⁶ Canadian Anonymization Network: Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’.

³²⁷ Canadian Anonymization Network: Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’ (bracket added).

³²⁸ Canadian Anonymization Network: Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’.

³²⁹ IPC: De-Identification Guidelines for Structured Data (“This document highlights the key issues to consider when de-identifying personal information in the form of structured data and it provides a step-by-step process that institutions can follow when removing personal information from data sets.”)

CANON describes as “highly regarded”.³³⁰ However, if a “flexible” definition of de-identified data focused on its end state is chosen, PIAC believes it must be accompanied by a rigorous framework for protecting the spectrum of de-identified information (see details below).

258. **Introduce statutory restrictions and permitted uses.** PIAC **recommends** that clear statutory rules – both restrictions and permitted uses – for de-identified information should be introduced. However, we believe the fundamental question is: how? Viewed in context of Ontario’s proposal for enhancing consent, the province appears to be considering adding an *exception to consent* for de-identified information *for certain prescribed purposes*. This appears to be partly consistent with GoC’s Proposals to Modernize PIPEDA, which include adding an exception to consent for use/disclosure of de-identified information “for certain prescribed purposes” and considering incorporating the “concept of pseudonymous information”.
259. **Permit narrow range of prescribed purposes.** If PIAC’s understanding of Ontario’s proposal is correct, then clarifying the role of consent in relation to de-identified data and what constitutes “prescribed purposes” are likely to be highly contested topics. PIAC **recommends** that:
- **Narrow range of prescribed purposes:** There should be a *narrow range* of prescribed purposes (i.e., acceptable practices for which de-identified data can be *used or disclosed* without consent) and these should correspond to the statutory categories of personal information along the spectrum of identifiability. Effectively, privacy protections would be risk-based. As noted, only truly de-identified information would be outside the scope of privacy legislation and thus, unprotected. Other categories of de-identified information could be exempted from consent but subject to a range and degree of other privacy principles (e.g., transparency, accountability, safeguarding), depending on their risk factor for re-identification. This approach could accommodate data trusts, if/when they are legislatively enabled (which we oppose at this time – see below).
 - **No consent exception for initial creation:** As detailed above, the consent exception should not apply to the initial *creation* of the de-identified data (i.e., consent must be obtained to de-identify in the first place).
260. **Introduce penalties for re-identification and prohibitions on targeting individuals.** In addition to the foregoing, PIAC **recommends** that penalties for re-identification and prohibitions on targeting individuals should be introduced.
261. This PIAC recommendation is supported by certain key stakeholders, including GoC. For example, GoC’s Proposals to Modernize PIPEDA, include introducing “penalties for re-identification” to address “increasingly sophisticated means to re-identify information that ostensibly appears to be non-personal” and prohibitions on targeting individuals. Our recommendation also aligns with proposed Canadian legislative regimes, specifically Quebec Bill 64, which empowers CAI to impose penal penalties for offences that include attempting to re-identify an individual without authorization where their information is de-identified.³³¹
262. **Require robust governance framework(s).** In addition to the foregoing, PIAC **recommends** that privacy legislation should require robust governance framework(s), appropriate to the risk-based spectrum of de-identified information. Whether and to what degree legislation should “enable” certain data governance models, particularly “Trust Agents”, especially “data trusts”, is addressed below.
263. **Incent self-regulation mechanisms, with caveats.** Ontario’s proposal for legislation to *incent* the use of self-regulation mechanisms, to promote effective and privacy-protecting de-identification practices, is addressed below in the context of PIAC’s recommendations on self-regulation mechanisms overall. Here, we simply note that Ontario’s proposal appears to align with GoC’s Proposals to Modernize PIPEDA, which discuss incentivizing the use of technical/operational standards and codes (including Codes of Practice) and acknowledge that in other countries, effective de-identification is promoted by self-regulation mechanisms

³³⁰ Canadian Anonymization Network: Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’.

³³¹ Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR.

(e.g., standards and codes [including Codes of Practice], decision-making frameworks, and voluntary certification systems).³³²

DATA TRUSTS: DO NOT LEGISLATIVELY ENABLE NOW (PREMATURE)

Ontario proposal: As noted, the Ontario government proposes to create a legislative framework to *enable the establishment of data trusts* “for privacy protective data sharing”.³³³ According to the Ontario consultation news release, “data trust” is defined as “a legal mechanism that enables an organization’s data to be governed by a trusted third party, to ensure the transparent and accountable use of that data. They operate under legal agreements that follow existing intellectual property and privacy protection laws”.³³⁴ According to the Ontario consultation paper³³⁵, data trusts are “emerging data governance models”, specifically “new models for privacy protective data sharing”, “where *personal information, de(-)identified personal information, or aggregate data*, can be shared among different actors or sectors”. In particular, data trusts “allow organizations to assign an individual as the custodian or steward for the data, agree on a standard set of rules for how data would be shared, and ensure that whoever has access to the trust uses the data in accordance with these rules”. Data trusts have benefits including “unlock(ing)” the “value of the data” and “promoting collaboration, economic development, and innovative solutions to societal issues”, specifically “to drive innovation for the public good, or for a common interest among specific organizations”. For this reason, “guidelines, principles or standards for the use of these trusts” would be established.

264. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should not enable data trusts at this time. Instead, Canadian governments should conduct a joint comprehensive study of *data governance* models – including but not limited to “Trust Agents” or “Trusted Data Exchanges” (especially but not only data trusts) – to identify one or more models that equitably captures and distributes the value of data while respecting individuals’ privacy. At that time, a dedicated public consultation should be launched to consider *whether and how to legislatively enable* the selected data governance model(s). This position is elaborated next.
265. **Data poses a governance problem.**³³⁶ Data – which, as noted, is “the new oil” (see infographic³³⁷ below) – poses a global governance problem: “The world is struggling to govern data. The challenge is to reduce abuses of all kinds, enhance accountability and improve ethical standards, while also ensuring that the maximum public and private value can also be derived from data.”³³⁸ Canada faces the same dilemma. According to GoC’s Proposals to Modernize PIPEDA: “data is the fuel to grow the Canadian data-driven economy”; there are “complex data flows involving numerous parties, often across borders”; “(a)lmost every organization is now in the data business in some way, resulting in a lack of clarity about who is accountable for personal information”; “there is increasing collaboration between public and private sectors (...) which raises concerns about accountability, appropriate use of data in the public interest, and access to data for public policy-making”; and, for these reasons, “the legislative frameworks that support this marketplace must be balanced and fit for purpose”. PIAC agrees, however we emphasize that these legislative frameworks must be appropriately balanced *against individuals’ (right to) privacy*.

³³² See e.g., Canadian Anonymization Network: Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’ (referencing Codes and frameworks in other jurisdictions, including the UK’s “Anonymisation Decision-Making Framework” and Australia’s “The De-Identification Decision-Making Framework”).

³³³ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

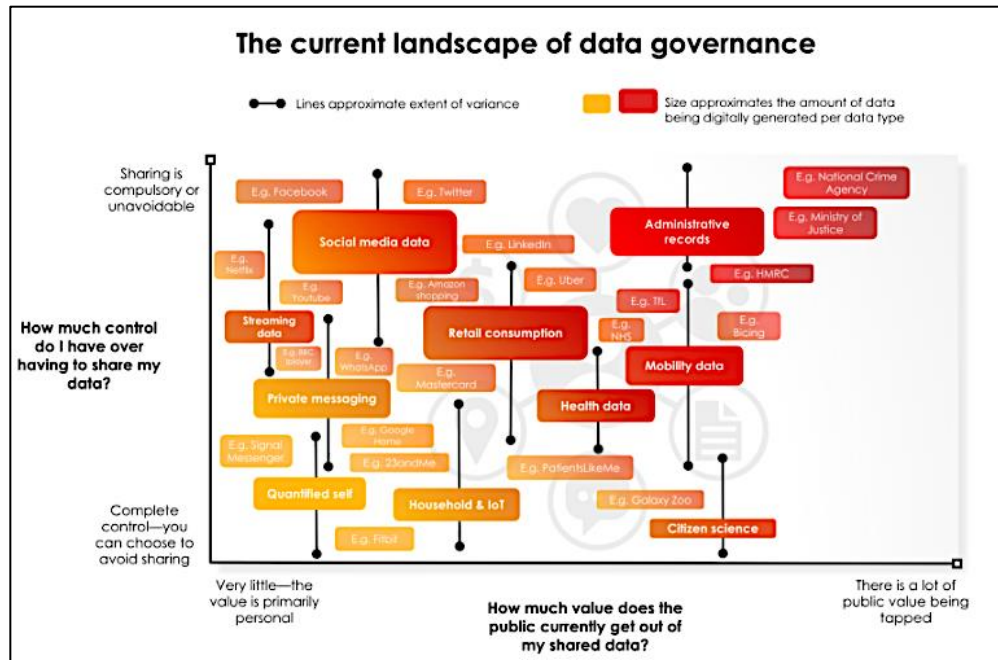
³³⁴ Ontario consultation news release, p. 3.

³³⁵ Ontario consultation paper, pp. 8-9 (emphasis added).

³³⁶ Data Trusts: Why, What and How; What is a data trust?; The New Ecosystem of Data Trusts.

³³⁷ The New Ecosystem of Data Trusts.

³³⁸ The New Ecosystem of Data Trusts.



266. **Plethora of data governance models.**³³⁹ There is a plethora of approaches to building governance over data (“data governance models”), including but not limited to “Trusted Agents” or “Trusted Data Exchanges” (e.g., “data trusts”), such as “data commons”, “data sharing pools”, “data repositories”, and “data cooperatives”. Many data governance models remain theoretical, have been implemented on an experimental basis only, or are still at early stages, making it difficult for policymakers to determine global best practice. This situation is confirmed by a January 2019 article by the Joint Research Centre, European Commission, Italy, entitled “The Governance of Data in a Digital Transformed European Society”³⁴⁰, which identifies “the lack of knowledge, and practical understanding, of alternative data governance models” as a “major challenge”:

“The mainstream paradigm in the current data landscape is based on the “data extraction” model typical of big online platforms, also defined [as] surveillance capitalism (Zuboff, 2015). However, this does not have to be the only way in which big data (and citizens’ personal data in particular) produce value. There is currently a debate among policy makers and academics about different forms of data governance (...) and a few experimental projects are being developed. However, we do not have yet matured and established models for sharing and adding value to data among all stakeholders: public sector, private sector, and the general public.”

This is particularly true for data trusts, since the biggest test case with the broadest mandate, the EU’s TRUSTS Project, is not expected to launch until 2023.

267. **“Data trust” definition is contested (legal v. functional).**³⁴¹ “Data trusts were first proposed by internet pioneer Sir Tim Berners Lee in 2018, and the concept has drawn considerable interest since then.”³⁴² However, “they are still relatively nascent in practice, certainly at scale, so defining them is a commercially and politically contested space”.³⁴³ In Canada, this was recently highlighted in the public debate over Sidewalk Lab’s “Civic/Urban Data Trust” proposal related to the Quayside Project in Toronto. In that

³³⁹ Emerging Models of Modern Data Governance; Data Commons & Data Trusts: What They Are and How They Relate; What is a Data Trust and Why are We Even Talking About It? Sidewalk Labs’ Magic Tricks.

³⁴⁰ The Governance of Data in a Digital Transformed European Society (square bracket added).

³⁴¹ The EU is launching a market for personal data; Trust; Wealth and Private Client: Trust Basics; Data Commons & Data Trusts: What They Are and How They Relate; Data Trusts: Why, What and How; What is a data trust?; The new ecosystem of data trusts; Affidavit of Sean McDonald in *CCLA v. Waterfront Toronto, et al*; Essential Requirements for Establishing and Operating Data Trusts.

³⁴² The EU is Launching a Market for Personal Data (emphasis and bracket added).

³⁴³ Affidavit of Sean McDonald in *CCLA v. Waterfront Toronto, et al*.

context, data trust expert Sean McDonald emphasizes that proponents of data trusts generally try to define the in two ways³⁴⁴:

- **Legal definition:** starting from the legal definition – “(d)ata trusts are legal trusts that manage data, or the rights to data”, a “contractual vehicle that can create fiduciary duties in digital spaces” – and “focusing on use cases that do, or could, use that model” (“legal data trust” or “data ‘trust’”); and
- **Functional definition:** “focusing on examples of models that do what a group functionally wants it to do, and calling those things a ‘trust’” (“functional data trust”).

Anouk Ruhaak, a Mozilla Fellow working with AlgorithmWatch researching data trusts and data governance models, contends that in light of this quandary “we might ask when something can be called a data trust. Is a data trust, by definition a trust that holds data rights? Or do we also include more hybrid forms?”³⁴⁵ To facilitate discussion without committing to exclusive definitions, working definitions have been proposed, such as “a data trust is a repeatable mechanism or approach to sharing data in a timely, fair, safe and equitable way”, chosen by a December 2019 working meeting of 15 Canadian organizations/initiatives involved in data sharing to fill the “gap in terms of practical guidance about how to establish and operate” one.³⁴⁶

268. **Ontario proposal appears to be for legal data trusts.** The Ontario government appears to be proposing a legal data trust model, consistent with GoC’s Proposals to Modernize PIPEDA, which assert that “(d)ata trusts treat datasets as the assets that an independent third party must manage according to contractual terms designed to ensure the responsible, appropriate use of those assets” and recommend that “de-identified information could be processed without consent when managed by a data trust”, for example, by revising the existing consent exception for research and statistical purposes in PIPEDA para. 7(3)(f).
269. **Little precedent or enabling legislation for legal data trusts.**³⁴⁷ Data “trusts” are important because they can be used “to experiment with data governance models, *with legal accountability*, in ways that de-risk data markets for industry and public interest users”, however “there are very few data trusts with such a broad mandate in existence” and “(a)s a result, *very little precedent or dedicated enabling legislation exists for how they might work in practice, or be held accountable by their beneficiaries*”.³⁴⁸
270. **Comparing data trusts to legal trusts is, at best, murky.**³⁴⁹ “Trusts” are defined as a *fiduciary relationship* created when property (“trust assets”) is transferred by one person (“settlor”) to another (“trustee”) to hold for the benefit of specified persons (“beneficiaries”).³⁵⁰ The rights to the property are divided, in that the trustee holds legal title while the beneficiary holds equitable title. The trustee’s job is to control, administer, and distribute the trust assets, for the beneficiaries’ benefit, according to the terms of the “trust agreement”³⁵¹ and applicable legal rules. The law imposes certain duties on trustees, including to: avoid conflicts of interest; *act exclusively for the benefit of beneficiaries and by corollary, never benefit from the trust*; act impartially as between beneficiaries (“maintain an even hand”); and account to the beneficiaries for the trust assets and the trust’s administration. While trusts can be created in different ways, “(t)he typical approach to creating a trust is that an owner donates an asset to a beneficiary”.³⁵² Trusts are “governance systems that support public *and* private benefit from shared resources”³⁵³ and, historically, they were applied to financial assets (e.g., pension funds) and real estate assets (e.g., public lands).

³⁴⁴ Affidavit of Sean McDonald in *CCLA v. Waterfront Toronto, et al.*

³⁴⁵ Data Commons & Data Trusts: What They Are and How They Relate.

³⁴⁶ Essential Requirements for Establishing and Operating Data Trusts.

³⁴⁷ Affidavit of Sean McDonald in *CCLA v. Waterfront Toronto, et al.* (emphasis added).

³⁴⁸ Affidavit of Sean McDonald in *CCLA v. Waterfront Toronto, et al.* (emphasis added).

³⁴⁹ The EU is Launching a Market for Personal Data; Trust; Wealth and Private Client: Trust Basics; Data Commons & Data Trusts: What They Are and How They Relate; Data Trusts: Why, What and How; What is a Data Trust?; The New Ecosystem of Data Trusts; Affidavit of Sean McDonald in *CCLA v. Waterfront Toronto, et al.*; Is Civic Data Governance the Key to Democratic Smart Cities?; Canada: Trust Basics.

³⁵⁰ Canada: Trust Basics. A trust is not a legal entity. Settlers are also referred to as “trustor(s)” and “grantor(s)”. There are different kinds of trust and, in some, the settlor can also be the trustee and/or beneficiary. However, the settlor cannot be the *sole* beneficiary.

³⁵¹ Defined as an agreement (oral or written) that identifies the parties and sets out the trustee’s rights and duties regarding the trust assets and beneficiaries.

³⁵² Affidavit of Sean McDonald in *CCLA v. Waterfront Toronto, et al.*

³⁵³ What is a data trust? (emphasis in original).

271. Proponents of data “trusts” (aka “fiduciary data trusts”³⁵⁴) view their purpose as pooling data from different sources (individuals and/or organizations [private/public]) (“data settlor”) and enabling an independent third party with a fiduciary duty to the trustor (“data trustee”), to negotiate on behalf of the settlor’s best interests with entities that access, use, or share the data (“data beneficiaries”). Effectively, this establishes “collective bargaining for data-sharing relationships”³⁵⁵:

“Fiduciary data trusts aren’t organizations; they’re contracts that give a trustee, or a group of trustees, authority to make decisions about how an asset — say, data — can be used on behalf of a group of people (...) (D)ata trusts are flexible and de facto global, meaning that they can be written in ways that create legally accountable governance structures. It’s helpful to think about a data trust as a container — one that can hold assets, define governance and manage liabilities. When used for governance, data trusts can steward, maintain and manage how data is used and shared — from who is allowed access to it, and under what terms, to who gets to define the terms, and how. They can involve a number of approaches to solving a range of problems, creating different structures to experiment with governance models and solutions in an agile way.”³⁵⁶

272. In contrast, opponents of data trusts contend that data “trust” is a term that “sound(s) legal but (is) very murky”³⁵⁷, because there are technical issues with applying the legal concept of a trust to data. One issue is the required element of “data assets/rights”. Sean McDonald emphasizes that “a defined property interest (...) is a requirement of the asset donation that creates a trust” and Anouk Ruhaak explains that:³⁵⁸

“In a data trust, the community places their data or data rights under the control of a trustee, or board of trustees. Similarly, the trustees have a fiduciary duty to look after the sole interest of the beneficiaries, which range from data subjects to those that need protection from data being abused. Data trusts can have many different purposes. Some might exist to make data available to academic researchers trying to cure cancer, others may ensure agricultural data is used for sustainable farming. Data trusts can be a great way to safeguard the privacy of one or many, but that does not mean they are always the right tool. In order for data trusts to be relevant we need to have a ‘thing’ (an asset or a right) that we can hand over to a board of trustees. When it comes to data that ‘thing’ is usually a right we have over the data. Various data protection laws around the world grant individuals rights over their data, such as the right to decide what data is shared and for which purpose. In addition, some data may be subject to intellectual property rights. As explained by Sylvie Delacroix and Neil Lawrence, those rights make data trusts possible: when we have rights over data we can hand over those rights to data trustees, to be held in a data trust. However, in many other cases, data does not have any rights attached to it. This is true, for instance, for a lot of the agricultural data described above. What do we do in those cases?”

In particular, according to Anna Artyushina, most Canadian jurisdictions do not recognize data as private property.³⁵⁹ Other technical issues with applying the legal concept of a trust to data are the trust elements of “asset owners” and “beneficiaries”. According to Mariana Valverde, Senior Fellow and Blogger, Digital Communities Advisory Panel, Professor at the University of Toronto Centre for Criminology and Sociolegal Studies, and expert on urban law and governance (writing about the Civic Data Trust proposed by Sidewalk Labs in Toronto):³⁶⁰

“(A) trust must have identifiable beneficiaries. That’s a problem, since nobody knows who could be the beneficiary of the proposed Sidewalk data trust: Waterfront Toronto itself? The City of Toronto? Waterfront residents? City residents? What about visitors whose data are harvested while sunbathing at Sugar Beach? Ordinarily a trust’s beneficiaries are either named individuals — the five grandchildren of Mr. Rich, say—or an identifiable group (such as patients receiving

³⁵⁴ What is a data trust?

³⁵⁵ What is a data trust?

³⁵⁶ What is a data trust? (brackets added; paragraph breaks deleted).

³⁵⁷ What is a Data Trust and Why are We Even Talking About It? Sidewalk Labs’ Magic Tricks (bracket added).

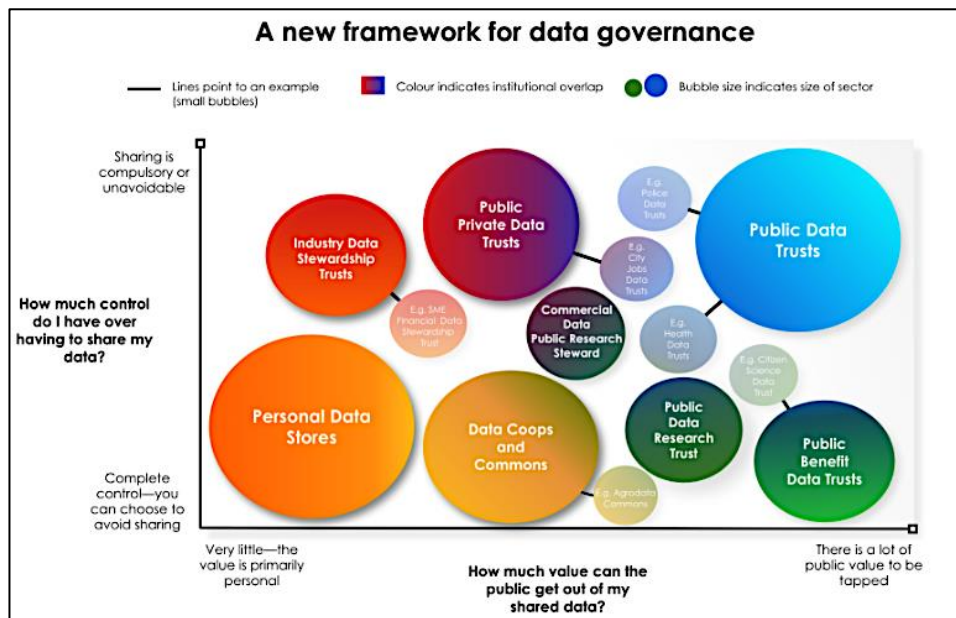
³⁵⁸ Data Commons & Data Trusts: What They Are and How They Relate (emphasis added, paragraph breaks deleted).

³⁵⁹ Is Civic Data Governance the Key to Democratic Smart Cities?

³⁶⁰ What is a Data Trust and Why are We Even Talking About It? Sidewalk Labs’ Magic Tricks (bracket added, paragraph breaks deleted).

services at a particular place). Canadian law can't tell us who would be the appropriate beneficiary for a data trust; but it does tell us that the owners of the assets are the ones who decide who the trustees will be. And Canadian law tells us something else that Sidewalk is hiding: that the general public is the one group that cannot be a beneficiary of any trust."

273. **Numerous data trust models.**³⁶¹ There is "no shortage of possible applications" of data trusts, however defined, including "industry data stewardship trusts" (business data), "public data trusts" (government data), and "public private data trusts" (government and business data) (see Infographic³⁶² below). Anna Artyushina explains that: "(D)ata trusts may serve different purposes: they can be for-profit enterprises, or they can be set up for data storage and protection, or to work for a charitable cause. IBM and Mastercard have built a data trust to manage the financial information of their European clients in Ireland; the UK and Canada have employed data trusts to stimulate the growth of the AI industries there; and recently, India announced plans to establish its own public data trust to spur the growth of technology companies."³⁶³



274. **Data trusts are not a panacea.**³⁶⁴ While data trusts – or at least, data “trusts” – hold promise, they are not a panacea. In the words of CIGI senior fellows Bianca Wylie and Sean McDonald: “(D)ata trusts aren’t a guarantee of anything. Using data trusts doesn’t inherently create good governance or solve the very real questions about the best business model for public interest data stewardship. They are one piece of a larger governance puzzle, one that necessarily includes laws, policies, standards, rights and much more.”³⁶⁵ PIAC believes that, *depending on what model(s) is adopted, data trusts could “change the privacy landscape on a global scale”³⁶⁶ for better or worse.* Overall, data trusts raise concerns about important issues including regulation, governance, and mis-use that have demonstrated, real-world impacts (see Table below).

Data Trust Concern	Details/Impacts
Regulation	Governments that intend to profit from data trusts are weakly positioned to regulate them because they are trapped in a conflict of interest, and therefore could “overlook the question of privacy”. ³⁶⁷

³⁶¹ The New Ecosystem of Data Trusts; The EU is Launching a Market for Personal Data.

³⁶² The New Ecosystem of Data Trusts.

³⁶³ The EU is Launching a Market for Personal Data (emphasis and bracket added).

³⁶⁴ The EU is launching a market for personal data; What is a Data Trust?

³⁶⁵ What is a Data Trust?

³⁶⁶ The EU is Launching a Market for Personal Data.

³⁶⁷ The EU is Launching a Market for Personal Data.

Governance	Data trusts do not automatically guarantee more transparency, because “(t)he trust is governed by a charter created by the trust’s settlor, and its rules can be made to prioritize someone’s interests” and “the trust is run by a board of directors, which means a party that has more seats gains significant control”. ³⁶⁸ “(C)ompanies that trade in personal data” (e.g., Big Tech) “cannot be trusted to store and manage it”, as demonstrated during the recent US Congressional antitrust hearing by the “four major platform companies” who “publicly recognized the use of surveillance technologies, market manipulation, and forceful acquisitions to dominate the data economy”. ³⁶⁹
(Mis-)Use	Data trusts can be improperly used, in ways that “actually deprive citizens of their rights to (control) their own data” and their privacy. ³⁷⁰ For example: “In October 2019, the government of Canada rejected a proposal by Alphabet/Sidewalk Labs to create a data trust for Toronto’s smart city project. Sidewalk Labs had designed the trust in a way that secured the company’s influence over citizens’ data. And India’s data trust faced criticism for giving the government unrestricted access to personal information by defining authorities as ‘information fiduciaries.’” ³⁷¹

Anna Artyushina contends it is “not yet clear” what model the EU TRUSTS Project will pursue, but “ideally” it “would show the world a more equitable way to capture and distribute the true value of personal data”, and “(t)here’s still time to deliver on that promise”³⁷² by its expected 2023 completion date.

275. **Data trusts are a “trojan horse” for AI battleground.** In particular, PIAC is concerned that data trusts are a “trojan horse” in the battle by Canadian governments (federal and PT) and private organizations to capture a portion of the increasingly lucrative world market for AI and machine learning, as alluded in the above table. Canadian governments, including Ontario, “should bear in mind that following Silicon Valley’s old motto to ‘move fast’ may actually ‘break things’ – and public trust is extremely fragile at the moment”³⁷³, in the midst of the COVID-19 pandemic. In this context, data trusts are comparable to digital contact tracing, which “holds promise” but “without the appropriate technological, legal, political and societal determinations, it can open the floodgates to relentless – and in a state of emergency, legitimized – data harvesting practices, persistent surveillance and a seismic shift in the balance of power between the individual, the state and private actors”.³⁷⁴
276. **Take wait-and-see approach to data trusts.** For the reasons outlined, PIAC **recommends** it would be prudent for Canadian governments (FPT) to take a wait-and-see approach to legislatively enabling data trusts so that a deliberate, informed decision can be made in future, based on a comprehensive study of data governance models, lived experience, and best practices in the EU and other countries that are conducting data governance – especially data trust – experiments. This cautious approach is not only warranted, but vital, since data trusts are being proposed as an exception to consent and it would be difficult if not impossible to put the proverbial toothpaste back in the tube.
277. **If data trusts are legislatively enabled, only permit with de-identification at source.** PIAC **recommends** that if data trusts are legislatively enabled, and excepted from consent, they should only be permitted if de-identification at the source is guaranteed.

³⁶⁸ The EU is Launching a Market for Personal Data.

³⁶⁹ The EU is Launching a Market for Personal Data.

³⁷⁰ The EU is Launching a Market for Personal Data (bracket added).

³⁷¹ The EU is Launching a Market for Personal Data.

³⁷² The EU is Launching a Market for Personal Data.

³⁷³ Digital Contact Tracing: The Trojan Horse in the Battle Over Data.

³⁷⁴ Digital Contact Tracing: The Trojan Horse in the Battle Over Data.

NECESSITY & PROPORTIONALITY: INTRODUCE

Ontario proposal: Silent.

278. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should explicitly require “necessity” and “proportionality” obligations if a rights-based privacy regime is adopted.
279. This PIAC recommendation is supported by certain key stakeholders, including Canadian privacy commissioners. For example, OPCC Annual Report 2019-20 emphasizes that “the principles of necessity and proportionality (...) are recognized globally as fundamental privacy principles but are not reflected in our federal laws”.

ACCOUNTABILITY: ENHANCE

Ontario proposal: Silent. However, the Ontario government proposes enhancing *specified* compliance and enforcement tools that would have the effect of strengthening accountability.

280. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance accountability, by introducing “demonstrable accountability”, meaning accountability that is demonstrated to the privacy regulator (see details below).
281. This PIAC recommendation is supported by certain key stakeholders, including Canadian privacy commissioners. For example, OPCC Annual Report 2018-19 proposes “stronger accountability requirements” in PIPEDA, specifically “demonstrable accountability”, to “help achieve truly meaningful privacy protection in a digital age”. The reason is that imposing accountability obligations and then letting organizations decide how they will comply “is another form of self-regulation, which has proven to be untenable” in cases including Facebook³⁷⁵ and Equifax.

DATA BREACH, TRANSFER (TO THIRD PARTIES/OTHER COUNTRIES) & LOCALISATION: ENHANCE & INTRODUCE

Ontario proposal: As noted, the Ontario government proposes to require organizations to report “substantial” privacy breaches. However, it is silent on personal data transfer – to third parties (“outsourcing”) and other countries – and on data localisation.

282. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance and introduce, as relevant, obligations regarding: data breaches; data transfers to third parties; data transfers to other countries; and data localisation, as follows.

DATA BREACH: ENHANCE

283. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance obligations regarding data breaches. The new PIPEDA data breach notification requirements are not sufficiently protective of individuals due to their likely ineffectiveness, extremely high threshold for notification, the determination of the seriousness of the breach being in the eye of the breaching organization, misaligned incentives for organizations, practical impossibility of auditing compliance, and lack

³⁷⁵ See details below, under “investigation and audit”.

of OPCC power to compel notification. PIPA AB, with its declarative structure and superior data breach notification regime, could be used as a model.

284. PIAC notes that Quebec Bill 64 proposes mandatory breach notification requirements going beyond GDPR, by covering breaches (“confidentiality incidents”) involving the unauthorized *use* of personal information (versus only access to, disclosure, or loss).³⁷⁶

DATA TRANSFERS TO THIRD PARTIES (“OUTSOURCING”): ENHANCE

285. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance obligations regarding data transfers to third parties, in ways including clarifying that organizations that transfer *de-identified* information to a third party remain accountable for its collection, use, and disclosure.

DATA TRANSFERS TO OTHER COUNTRIES: ENHANCE

286. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance obligations about data transfers to other countries (aka “international transfers”), to ensure that Canadians’ personal information is properly protected when it leaves Canada.
287. In particular, PIAC **recommends** enhancing obligations about international transfers by:
- requiring consent to transfer personal information outside Canada;
 - adopting demonstrable accountability; and
 - considering adding to, or replacing, the “comparable level of protection” standard with mechanisms that exist under GDPR and other jurisdictions (e.g., EU’s SCCs, codes of conduct, or other binding schemes) or that have been proposed (e.g., the concept of “data fiduciary” in the proposed *New York Privacy Act* [“NYPA”]³⁷⁷).
288. These PIAC recommendations are supported by certain key stakeholders, including Canadian privacy commissioners. For example, OPCC Annual Report 2019-20 warns that PIPEDA’s current standard “does not adequately address risks to privacy posed by global data flows”, as proven by its Equifax investigation, and thus “likely” needs to be strengthened in ways that could include the aforementioned existing and proposed global transfer mechanisms.
289. However, if new Ontario legislation is introduced, PIAC **opposes** introducing a GDPR-style “adequacy” condition that requires assessment of jurisdictions’ (countries’ or PTs’) privacy protections, modelled on Quebec’s Bill 64, pursuant to which the Quebec government is expected to publish a list of “States” (uncertain definition) whose legal framework governing personal information is “equivalent” to Quebec’s.³⁷⁸ As noted, former federal privacy commissioner Jennifer Stoddart warns this process has proved cumbersome to even the EU’s large, experienced bureaucracy. Further, it could have significant negative impacts on international and inter-PT data flows/trade and, as CMA cautions, it is important to ensure that Bill 64’s “measures are proportionate to the privacy goals at hand, without causing unnecessary complexity for consumers and businesses”.³⁷⁹

³⁷⁶ Quebec Plans Ambitious Overhaul of its Privacy Law.

³⁷⁷ See e.g., Implications of the ‘Data Fiduciary’ Provision in the Proposed New York Privacy Act (explaining that “entities collecting and controlling data would owe fiduciary duties to the individuals from which the data was collected” and “these obligations would include ‘the duty of care, loyalty and confidentiality,’ as well as the requirement to ‘act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.”)

³⁷⁸ Bill 64 requires that information can only be transferred or disclosed to a “State” (silent on whether PTs count) outside Quebec if: a privacy assessment is conducted that establishes the information would receive the same level of protection as provided under Quebec’s privacy laws; and there is a written agreement to ensure accountability: Quebec Bill 64, s. 103. See also: Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business; Canada: Bill 64: Modernizing Quebec’s Privacy Regime; Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

³⁷⁹ Privacy Update – Provincial Privacy Law Reform, Final CCPA Regulations and More.

DATA LOCALIZATION: INTRODUCE, SUBJECT TO INTERNATIONAL TRADE AGREEMENT RESTRICTIONS

290. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce data localization obligations regarding data transfers to other countries. However, we acknowledge that introducing a federal or Ontario data localization requirement could face challenges, including restrictions in international trade agreements (e.g., pursuant to the *Comprehensive and Progressive Trans-Pacific Partnership* [“CPTPP”] and *Canada-US-Mexico Agreement* [“CUSMA”]).³⁸⁰
291. A data localization requirement would align with existing international and Canadian legislative regimes. For example, globally, outside the EU, there is an “increasing trend of national data localization rules”, and Alberta and QC have data localization provisions in their private sector privacy statutes.³⁸¹

INDIVIDUAL RIGHTS: INCREASE & ENHANCE

Ontario proposal: As noted, the Ontario government effectively proposes to enhance the right to withdraw consent and explicitly proposes to introduce two specific data rights, the right to erasure/be forgotten and the right to data portability (see details below). However, it is otherwise silent on individual rights.

292. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should adopt a rights-based approach and increase the number and scope of individual rights, as follows.

RIGHTS-BASED APPROACH: INTRODUCE

Ontario proposal: Silent.

293. As noted, PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should adopt a “human rights-based approach to privacy”³⁸² that is embedded in a new Preamble and purpose statement.
294. This PIAC recommendation is supported by certain key stakeholders, including GoC and privacy commissioners (Canadian and international). For example, the December 2019 ISED Minister Mandate Letter directs the Minister to establish “a new set of online rights”. OPCC Annual Report 2018-19 and 2019-20 propose to modernize PIPEDA by adopting a “rights-based approach” (aka “rights-based privacy law”). In October 2019, at the International Conference of Data Protection & Privacy Commissioners (“ICDPPC”), since renamed Global Privacy Assembly (“GPA”), members adopted an OPCC-sponsored and drafted “Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising other Fundamental Rights”³⁸³, which “was an important step in the commitment to privacy as a human right worldwide”³⁸⁴.
295. A rights-based approach to privacy legislation would also align with most of Canada’s trading partners, including the EU, pursuant to GDPR (see Table in Part 2). The fact that EU businesses “are continuing to operate successfully under the GDPR” demonstrates that “(r)ights-based laws are not an impediment to innovation” and “(t)o the contrary, they help to build the consumer trust necessary to support and drive an efficiently operating digital economy”.³⁸⁵

³⁸⁰ See e.g., Chapter 8: Trans-border Data Flows and Data Localization Requirements in *Big Data Law in Canada*.

³⁸¹ Chapter 8: Trans-border Data Flows and Data Localization Requirements in *Big Data Law in Canada*. BC and NS have data localisation provisions in their *public* sector privacy legislation.

³⁸² OPCC Annual Report 2018-19; OPCC Annual Report 2019-20.

³⁸³ ISED’s Sixth Update Report on Developments in Data Protection Law in Canada: Report to the European Commission December 2019.

³⁸⁴ OPCC Annual Report 2019-20.

³⁸⁵ OPCC Annual Report 2019-20.

296. In particular, PIAC **recommends** that the statutory rights-based approach to privacy should, consistent with OPCC’s proposals in Annual Report 2018-19 and 2019-20, protect privacy as both:³⁸⁶
- **A fundamental human right:** defined broadly, to align with SCC jurisprudence and recognize the quasi-constitutional nature of privacy laws, specifically as the *freedom to live and develop free from unjustified surveillance (by businesses and public organizations)*.
 - **A precondition:** for protecting and exercising other human rights, such as equality rights (“in an age when machines and algorithms make decisions about us”) and democratic rights (“when technologies can thwart democratic processes”).

RIGHT TO BE INFORMED: INTRODUCE

Ontario proposal: Silent.

297. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce the right to be informed about how personal information is being used, specifically the right to ask an organization to demonstrate its compliance with the *claimed* purposes (and therefore, its *actual* collections uses, and disclosures).
298. This PIAC recommendation is supported by certain key stakeholders, including GoC. For example, the December 2019 ISED Minister Mandate Letter directs the Minister to establish a new set of online rights “including (...) the knowledge of how personal data is being used, including with a national advertising registry”.
299. A right to be informed would align with existing international legislative regimes (e.g., GDPR).

RIGHT TO ACCESS: ENHANCE

Ontario proposal: Silent.

300. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance the right to access, by granting a specific right to access personal information that is used as the basis for algorithmic processing (see details below).

RIGHT TO RECTIFICATION: ENHANCE

Ontario proposal: Silent.

301. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance the right to rectification, by granting a specific right to correct personal information that is used as the basis for algorithmic processing (see details below).

³⁸⁶ Canada: Modernizing Federal Privacy Laws: Suggested Approaches of the Federal Government and the OPC; OPCC Annual Report 2018-19; OPCC Annual Report 2019-20; OPCC News release: Commissioner’s Annual Report Sets out Blueprint for How to Modernize Canadian Privacy Law; September 2020 OPCC Appearance on Quebec’s Bill 64 (referencing OPCC Annual Report 2018-19).

RIGHT TO RESTRICT & OBJECT TO PROCESSING (OVERALL): INTRODUCE

Ontario proposal: Silent.

302. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce the right to restrict processing (i.e., personal data may only be held by the initial organization and only be used for limited purposes) and to object to processing (e.g., to object to processing on certain alternative bases to consent [if these are created]). In addition to these overall rights, we recommend granting the specific right to object to algorithmic processing and enhancing the specific right to object to marketing (see details below).
303. This PIAC recommendation is supported by certain key stakeholders, including GoC. For example: the December 2019 ISED Minister Mandate Letter directs the Minister to establish a new set of online rights “including (...) the ability to review and challenge the amount of personal data that a company or government has collected”.
304. A right to restrict and object to processing would also align with existing international legislative regimes (e.g., GDPR).

RIGHT TO OBJECT TO MARKETING: ENHANCE

Ontario proposal: Silent.

305. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance the right to object to marketing, by granting the right to withdraw consent for the sale of personal information and for use of personal information for commercial prospecting purposes (see details below).

RIGHT TO WITHDRAW CONSENT: ENHANCE

Ontario proposal: As noted, the Ontario government effectively proposes to enhance the right to withdraw consent, by proposing “allowing individuals to revoke consent at any time”.

306. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance the right to withdraw consent, in the following ways.
307. PIAC **recommends** that legislation should permit withdrawal of consent *at any time* (i.e., without limits) and require withdrawal to be easy, or at least, as easy to withdraw consent as to give it. This would align with GDPR.
308. PIAC **recommends** that legislation should grant the following specific rights to withdraw consent: right to withdraw consent for the sharing or sale of data; right to withdraw consent for use of personal information for commercial or philanthropic prospecting purposes; and right to withdraw consent to automated processing and decision-making (see details below).
309. This PIAC recommendation is supported by certain key stakeholders, including GoC and Canadian privacy commissioners. For example, the December 2019 ISED Minister Mandate Letter directs the Minister to establish a new set of online rights “including (...) the ability to withdraw consent for the sharing or sale of data”. The OPCC, in its January 2020 Proposals for Ensuring Appropriate Regulation of Artificial

Intelligence³⁸⁷ under PIPEDA, states that it “view(s) integrating a right to object and to be free from automated decisions as analogous to the right to withhold consent”.

310. The right to withdraw consent for use of personal information for commercial or philanthropic prospecting purposes would align with proposed Canadian legislation. For example, Quebec Bill 64 provides such a right, which requires an organization that uses personal information for commercial or philanthropic prospecting purposes to identify itself to the individual and inform them of the right to withdraw consent, and once withdrawn, the use must stop.³⁸⁸
311. Finally, PIAC **recommends** that if legislation adopts alternative bases to consent (instead of exceptions to consent), then it should prohibit organizations from silently migrating to another legal basis to continue processing the personal information after consent is withdrawn. This too would align with GDPR.

RIGHT TO BE FORGOTTEN/ERASURE: INTRODUCE

Ontario proposal: As noted, the Ontario government proposes to *introduce a right for individuals to request information related to them be deleted or de-indexed* (aka “right to erasure” or “the right to be forgotten”), subject to limitations.³⁸⁹ According to the Ontario consultation paper³⁹⁰, the right to be forgotten allows individuals to permanently de-index (defined as removing from online search results or references) or delete personal information, and can be exercised where an individual has withdrawn consent or the collection was illegal. The right would be limited, but specific limits are not proposed, and GDPR limits are provided as examples (e.g., where the information is needed to exercise the right to freedom of expression, comply with legal obligations, perform tasks in the public interest, or exercise official authority). The right can only be limited for “reasons of public interest” (e.g., public health, archiving, research [scientific, historical, or statistical]) or legal claims (e.g., establishment, exercise, or defense).

312. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce the right to be forgotten/erasure, specifically to delete (“source takedown”) and de-index (subject to the pending Federal Court decision on the federal government’s jurisdiction over search engines³⁹¹). We agree with the Ontario consultation paper’s assertion³⁹² that a right to erasure “has become increasingly relevant in an era of digital services; it empowers individuals to manage their privacy and reputation more directly” in an environment where permanently posted online personal information can seriously damage individuals’ lives and livelihoods (i.e., cause “reputational harm”). Further, as noted, this right is a GDPR centrepiece.³⁹³
313. This PIAC recommendation is supported by certain key stakeholders, including GoC and Canadian privacy commissioners. For example, the December 2019 ISED Minister Mandate Letter directs the Minister to establish a new set of online rights “including (...) the ability to withdraw, remove and erase basic personal data from a platform”. OPCC Annual Report 2018-19 recommends that PIPEDA should introduce the “right to (...) removal or amendment of information at the source” and the “right to ask search engines to de-index web pages that contain inaccurate, incomplete or outdated information” (notwithstanding the “preliminary jurisdictional issue is currently before courts”, because it is “incumbent on Parliament to consider the right to be forgotten and other proposed remedies for protecting online reputation, and (...) it would be inappropriate to wait to act on such fundamental issues”).

³⁸⁷ Consultation on the OPC’s Proposals for Ensuring Appropriate Regulation of Artificial Intelligence.

³⁸⁸ Quebec Bill 64, s. 111. See also: Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business.

³⁸⁹ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

³⁹⁰ Ontario consultation paper, p. 5.

³⁹¹ At the date of writing, the question whether GoC has jurisdiction over search engines is under consideration by the Federal Court in the OPCC-initiated *Google Reference (T-1779-18)*, regarding a public complaint against Google requesting that certain web pages be de-indexed from results for searches of the complainant’s name. Remaining steps are for the parties and interveners to file their written arguments and for a hearing to be held. OPCC has indicated it will not finalize its “Draft Position Paper on Online Reputation” until the proceeding concludes. See OPCC Annual Report 2019-20.

³⁹² Ontario consultation paper, p. 5.

³⁹³ GDPR, art. 17.

314. A right to be forgotten would also align with proposed Canadian legislative regimes, notably Quebec’s Bill 64, which introduces a right to erasure that³⁹⁴:
- requires organizations to destroy or anonymize personal information when the purposes for which it was collected/used are achieved; and
 - grants individuals the right to require organizations to stop distributing personal information, or de-index any hyperlink connected to their name, if continued distribution would: injure their privacy rights or reputation; the injury is “clearly greater” than the public interest in free expression or knowing the information; and stopping dissemination would “not exceed what is necessary” to prevent the injury.
315. Further, PIAC **recommends** that the right to be forgotten should be limited, as the Ontario consultation paper proposes³⁹⁵, so that it does not become “impractical” for private organizations to follow. This aligns with GoC’s Proposals to Modernize PIPEDA by considering an explicit right to delete or de-index³⁹⁶ personal information *with some caveats*. In particular, we **recommend** adopting similar limits to those under GDPR, which provides a list of circumstances where an organization is not required to erase personal data, including: exercising freedom of expression, complying with a legal obligation, archiving (e.g., for research purposes), and public health reasons.³⁹⁷
316. PIAC also **recommends** requiring organizations to notify their deletion of personal information to any other organizations to which it was disclosed. Organizations should bear this burden because there is no way for individuals to identify the parties to which an organization has shared personal data. Such a responsibility is congruent with PIPEDA requirements for subcontracting or sub-processing personal information in Schedule 1, Principle 4.1.3.
317. This PIAC recommendation is supported by certain key stakeholders, including GoC. For example, GoC’s Proposals to Modernize PIPEDA include requiring organizations to communicate deletion of personal information to any other organization to which it was disclosed.
318. Finally, PIAC **recommends** defined retention periods. This PIAC recommendation is also supported by certain key stakeholders, including GoC. For example, GoC’s Proposals to Modernize PIPEDA include considering “use of defined retention periods”, in order “to increase data integrity and decrease the risk of misuse”.

RIGHT TO DATA PORTABILITY: INTRODUCE

Ontario proposal: As noted, the Ontario government proposes to *introduce a right for individuals to obtain their data in a standard and portable digital format*, giving them greater freedom to change service providers without losing their data (aka “data portability”).³⁹⁸ According to the Ontario consultation paper³⁹⁹, the right to data portability requires organizations to, upon request, provide individuals with their personal information in an “open, accessible format” (“and possibly standardized form”) and includes the ability for individuals to move all of their data from one private organization (e.g., “a social media platform”) to another (aka “vote with their feet”).

319. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce the right to data portability, specifically for individuals to direct that their personal information be moved from one organization to another in a standard and portable digital format. We agree with the Ontario consultation paper’s assertion⁴⁰⁰ that the right to data portability not only benefits consumers by enabling them to choose alternative service providers with better service(s) or privacy protections (without losing all

³⁹⁴ Torys: Ontario Enters the Private Sector Privacy Realm.

³⁹⁵ Ontario consultation paper, p. 5.

³⁹⁶ GoC’s Proposals to Modernize PIPEDA emphasize that the right to de-index depends on whether the Federal Court decides that PIPEDA applies to search engines in the *Google Reference*.

³⁹⁷ GDPR, art. 17 ¶3.

³⁹⁸ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

³⁹⁹ Ontario consultation paper, p. 6.

⁴⁰⁰ Ontario consultation paper, p. 6.

their personal data), but also benefits service providers, by creating greater competition and fostering innovation.

320. This PIAC recommendation is supported by certain stakeholders, including GoC. For example, the December 2019 ISED Minister Mandate Letter directs the Minister to establish a new set of online rights “including data portability”, and GoC’s Proposals to Modernize PIPEDA include introducing an explicit right to data portability (aka “mobility”), citing studies in other jurisdictions showing that data portability has potential to enhance consumer choice, facilitate growth of innovative goods and services, and encourage competition.⁴⁰¹
321. A right to data portability would also align with existing and proposed Canadian legislative regimes. For example, Quebec’s existing private sector privacy legislation requires an organization that holds a file on an individual to, upon request, confirm the file exists and communicate to them any personal information, and Bill 64 broadens this right, by allowing the individual to obtain a copy of the information in a written, intelligible transcript, and to request “computerized” information, in a structured, commonly used technological format.⁴⁰²
322. We note that GoC’s Proposals to Modernize PIPEDA ask, but do not answer, the question of whether the right to data portability should extend to *both* derived and 3rd party information. PIAC **recommends** that the right to data portability should include “derived information” and, possibly, “3rd party information” (defined as personal information pertaining to a third party, such as the individual’s contact list).
323. Additionally, PIAC **recommends** that the right to data portability should have caveats (i.e., exceptions), as stated in GoC’s Proposals to Modernize PIPEDA, specifically where it would be “contrary to law enforcement principles, prejudice an investigation, would reveal proprietary processes or technologies, or where it is not technically feasible”.
324. Notwithstanding the above, PIAC **recommends** that a cautionary approach should be taken in designing the right to portability, to ensure that any privacy risks *posed by it* (e.g., fraud) are appropriately mitigated. This could be achieved through a phased-in, sector-by-sector approach.

RIGHT TO REQUEST SOURCE OF INFORMATION: INTRODUCE

Ontario proposal: Silent.

325. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce a right to request the source of information, in situations where organizations collect personal information from another individual or organization, whereupon the organization must inform the individual of the data source.
326. This PIAC recommendation would align with proposed Canadian legislative regimes, specifically with Quebec Bill 64, which creates such a right.⁴⁰³
327. Further, to facilitate implementation of the right to request the source of information, PIAC **recommends** that legislation should require an organization that obtains personal information about an individual from a third party to note the source in the individual’s file.

RIGHTS RELATED TO AUTOMATED DECISION-MAKING & SURVEILLANCE: INTRODUCE

⁴⁰¹ GoC’s Proposals to Modernize PIPEDA.

⁴⁰² Quebec Bill 64, s. 112. See also: Torys: Ontario Enters the Private Sector Privacy Realm; Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business; Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR; Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

⁴⁰³ Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR; Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

Ontario proposal: Silent.

328. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce rights related to automated decision-making and surveillance (e.g., profiling). We agree with the late Ian Kerr, former Canada Research Chair in Ethics, Law, and Technology, and former member of Canada’s Advisory Council on Artificial Intelligence that: “we stand on the precipice of a society that increasingly interacts with machines, many of which will be more akin to agents than mere mechanical devices. If so, our laws need to reflect this stunning new reality.”⁴⁰⁴
329. In particular, PIAC **recommends** that legislation should introduce the following specific rights related to automated decision-making and surveillance (subject to certain exceptions) and, to help clarify them, a definition of “artificial intelligence” that distinguishes between the key terms of AI, ML, and big data analytics, which OPCC notes “are often used interchangeably but have subtle differences”⁴⁰⁵:
- **Right to be free from automated processing:** right to be free from automated processing (i.e., without having to object), including profiling.
 - **Right to know about, and deactivate, profiling:** requirement for an organization using technology that has the ability to identify, locate, or profile an individual to inform them of said technology and the means available, if any to deactivate it. This would be an adjunct to PIAC’s previous recommendation for algorithmic transparency and especially impact the ad tech industry and its users.
 - **Right to object to automated processing:** right to object to automated processing of one’s personal information, including:
 - Right to be informed about the use of automated decision-making
 - Right to object to automated decision-making (effective immediately) or to request human intervention
 - Right to correct personal information used to make automated decisions
 - Right to explanation on (i.e., reasons for) automated decisions, including factors and their weight
 - Right to object to automated decisions
 - Right to withdraw from being the subject of automated decisions
 - **Right to be free from algorithmic discrimination and bias:** the right to be free from “algorithmic discrimination and bias”, operationally defined as “systematic and repeatable errors in a computer system that create unfair outcomes, such as privileging one arbitrary group of users over others”.⁴⁰⁶
330. These PIAC recommendations are supported by certain key stakeholders, including GoC and Canadian privacy commissioners. For example, the December 2019 ISED Minister Mandate Letter directs the Minister to establish a new set of online rights “including (...) the ability to be free from online discrimination including bias and harassment”. OPCC Annual Report 2018-19 recommends that PIPEDA should “incorporate rights that protect against harms that are unique to the digital era, including but not limited to ubiquitous surveillance, discrimination in profiling, automated decision-making, and behavioural data analytics”. In early 2020, OPCC launched a public consultation on protecting Canadians’ privacy rights as AI expands, including, as noted, a discussion paper containing key proposals for PIPEDA reform, because “(t)heir use for making predictions and decisions affecting individuals may introduce privacy risks and discrimination” which must be mitigated by “clear rules” that protect human rights including but not limited to privacy.⁴⁰⁷ As of October 2020, OPCC is considering stakeholder input, which “will serve to refine our thinking and make our law reform proposals more relevant”.⁴⁰⁸

⁴⁰⁴ Robots and Artificial Intelligence in Health Care, p.257.

⁴⁰⁵ Consultation on the OPCC’s Proposals for Ensuring Appropriate Regulation of Artificial Intelligence.

⁴⁰⁶ Wikipedia: Algorithmic bias.

⁴⁰⁷ OPCC Annual Report 2019-20.

⁴⁰⁸ OPCC Annual Report 2019-20.

331. Rights related to automated decision-making and surveillance would also align with existing international legislative regimes (e.g., GDPR⁴⁰⁹) and proposed Canadian legislative regimes, specifically Quebec Bill 64, which provides a new framework for automated decision-making. The framework includes:
- **Right to object to automated processing:**⁴¹⁰ requires an organization to *inform* an individual of its intent to render a decision based exclusively on automated processing of personal information, the personal information used to render the decision, the reasons for the decision, and the right to have the personal information corrected; and grants the individual the right to *object* to the decision.⁴¹¹ Notably, this right does not go as far as GDPR, because it does not grant the right to *withdraw* from being the subject of the decision.⁴¹²
 - **Rights in relation to profiling:**⁴¹³ requires organizations that collect personal information using technology that allows an individual to be “identified, located, or profiled” to inform the individual of such use and of the means available, if any, to deactivate that function. “Profiling” is defined as the collection and use of personal data to assess an individual’s characteristics for the purpose of analyzing their work performance, economic situation, health, personal preferences, interests, or behaviour.

CHILDREN’S RIGHTS (OVERALL): INTRODUCE

Ontario proposal: Silent.

332. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should effectively introduce a children’s right to privacy, by introducing a set of privacy protections that pertains only to individuals aged 0-16 . Children are a unique and vulnerable group of users which deserves special privacy protections. Boys and Girls Clubs of Canada President and C.E.O. Owen Charters has urged policy makers to make children's privacy rights a priority in Canada.⁴¹⁴
333. In particular, PIAC **recommends** that, at minimum, the following types of protections for individuals aged 0-16 should be introduced:
- **Privacy notices:** Services offered to children must ensure privacy notices are written in a plain, clear way that a child would understand.⁴¹⁵
 - **Consent:** Consent for collecting or processing of any data of a child must be given by a parent.⁴¹⁶
 - **Prohibition on automated data processing:** Children should not be subject to automated data processing (e.g., profiling and behavioural advertising).⁴¹⁷
 - **Right to erasure:** Children have a greater right to erasure of their personal data collected while they were children. This right survives in regard to such data when the data subject reaches the age of majority or the age designated by the relevant privacy statute.⁴¹⁸ For example, PIAC has called for personal data collected from children to no longer be retained by websites once the child reaches 18, unless the newly adult child explicitly consents to the website carrying this information forward (a “get

⁴⁰⁹ See e.g., PIPEDA v. GDPR: The Key Differences, and analysis in Part 2 of this submission.

⁴¹⁰ Quebec Bill 64, s. 102.

⁴¹¹ Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business.

⁴¹² Canada: Bill 64: Modernizing Quebec’s Privacy Regime.

⁴¹³ Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime; Quebec to Introduce the Most Punitive Privacy Laws in Canada; Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR.

⁴¹⁴ Canada Can Do More to Protect Our Children Online.

⁴¹⁵ Aligned with GDPR, recital 58.

⁴¹⁶ Aligned with GDPR, art. 8.

⁴¹⁷ Aligned with GDPR, recital 71.

⁴¹⁸ Aligned with GDPR, recital 65, in particular: “The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.”

out of marketing jail free card”) so that they “will have control when they start their adult life without the marketing baggage they collected just to play online or socialize with friends”.⁴¹⁹

334. Statutory protections for individuals aged 0-16 would align with existing and proposed international and Canadian legislative regimes. For example, GDPR, as noted, has recognized the special status of children’s privacy rights by creating specific rules that apply to children aged 16 or under (allowing Member States to adjust the age requirement from 13-16). Quebec’s Bill 64 creates new provisions for children under 14, requiring express consent from the individual with parental authority.⁴²⁰

OVERSIGHT, COMPLIANCE & ENFORCEMENT: STRENGTHEN

Ontario proposal: As noted, the Ontario government proposes to *increase oversight, compliance, and enforcement powers* for the Ontario Privacy Commissioner, to ensure businesses comply with the law, including the ability to impose penalties.⁴²¹ According to the Ontario consultation paper⁴²², it is important to couple a “proactive, positive approach to compliance” involving tools and strategies that “assist and encourage organizations to observe” privacy rules (“compliance tools”) with tools and strategies that enforce privacy rules (“enforcement tools”), which *could* include:

Compliance Tools

- Expanded mandate for IPC to provide advice/guidance to private organizations (e.g., identify best practices for making them more privacy protective), in the form of education, research, guidance, advisory services and “regulatory sandboxes”, that is not “one size fits all” but rather tailored to small, medium, and large organizations.

Enforcement Tools

- Power to issue binding orders to organizations found to have violated privacy rules (“order-making power”) and to impose penalties for non-compliance, including to levy fines “in severe cases”.
- Power to issue non-binding recommendations and public reports about an organization’s privacy practices.
- Power to process public complaints, initiate investigations, require organizations to report “substantial” privacy breaches, and “take public action in response to privacy investigations”.

335. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should strengthen oversight, compliance, and enforcement.
336. This PIAC recommendation is supported by certain key stakeholders, including GoC. For example, the December 2019 ISED Minister Mandate Letter directs the Minister to advance “enhanced powers” for the Canadian Privacy Commissioner. GoC’s Proposals to Modernize PIPEDA recognize that “(t)here are currently constrained consequences and impacts on organizations for non-compliance with PIPEDA” particularly “lack of consequences for egregious behaviour” and: “There is a growing view that the ombudsman model and enforcement of PIPEDA, which relies largely on recommendations, naming of organizations in the public interest, and recourse to the Federal Court, to effect compliance with privacy laws, is outdated and does not incentivize compliance, especially when compared to the latest generation of privacy laws. The current state of affairs cannot continue...”⁴²³ Further, the GoC Proposals emphasize that “(a)n effective enforcement regime generally involves activities related to four components” (see diagram):

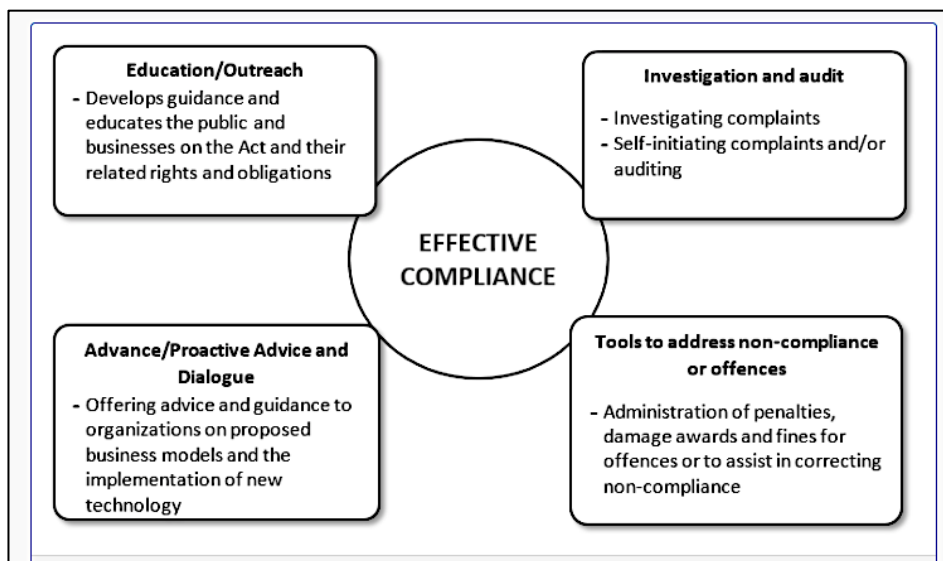
⁴¹⁹ Children’s Privacy Threatened by Play Websites and Social Networking.

⁴²⁰ Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR.

⁴²¹ Ontario consultation news release, p. 3; Ontario consultation paper, p. 3.

⁴²² Ontario consultation paper, pp. 6-7.

⁴²³ GoC’s Proposals to Modernize PIPEDA.



337. For these reasons, PIAC **recommends** empowering OPCC (and PT privacy commissioners) with a full array of oversight, compliance and enforcement tools, including *all* of the potential tools identified by the Ontario government *plus* additional PIAC-recommended tools (see below). Together, these tools would, in the words of the Ontario consultation paper⁴²⁴, “ensure that (private) organizations remained compliant in upholding the privacy rights of individuals” and “support the public’s confidence that enforcement is meaningful, and therefore encourage good privacy practices among commercial actors”.
338. We note our expectation that, notwithstanding enhanced enforcement tools, Canadian privacy commissioners will maintain their belief that "enforcement should not be the primary strategy to seek compliance" and continue to prefer "proactive efforts", meaning "addressing privacy issues upfront and resolving matters cooperatively, outside formal enforcement".⁴²⁵

COMPLIANCE TOOLS: ENHANCE

Ontario proposal: As noted, the Ontario government proposes to increase IPC’s power by way of compliance tools, which could include an expanded mandate for IPC to provide advice/guidance to private organizations (e.g., identify best practices for making them more privacy protective), in the form of education, research, guidance, advisory services and “regulatory sandboxes”, that is not “one size fits all” but rather tailored to small, medium, and large organizations.

339. In addition to the Ontario-proposed compliance tools, PIAC **recommends** empowering OPCC (and PT privacy commissioners) with the following PIAC-recommended tools.

“DEMONSTRABLE” ACCOUNTABILITY: INTRODUCE

Ontario proposal: Silent.

⁴²⁴ Consultation paper, p. 7 (bracket added).

⁴²⁵ OPCC Annual Report 2018-19.

340. As noted, PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce “demonstrable accountability”, defined by OPCC as the legal power of a data protection authority to *seek production of specific records* to prove data management practices, prior to investigation, and/or to *conduct proactive* inspections, reviews, and audits to verify compliance, absent specific grounds to suspect or believe a specific infraction has occurred.⁴²⁶
341. This PIAC recommendation is supported by certain stakeholders, including Canadian privacy commissioners. For example, as noted, OPCC Annual Report 2018-19 proposes revising PIPEDA to require demonstrable accountability. According to the Report, demonstrable accountability is: especially important when *unconsented* collection, use, and disclosure is permitted, and organizations are “expected to fill the protective void through accountability”; and “part of the solution in protecting Canadians in the context of transborder data flows” (a hard lesson learned from the recent Equifax case). The October 2019 Joint Resolution of FPT Privacy Commissioners calls for commissioners to have “the power to compel records and witnesses as necessary for reviews and investigations” and to “conduct own-motion investigations and audits”.
342. Demonstrable accountability would also align with most of Canada’s trading partners, including the EU, pursuant to GDPR (see Table in Part 2).
343. Further, PIAC **recommends** that demonstrable accountability should be implemented in ways that include certain enhanced compliance tools (e.g., required record-keeping) and enforcement tools (e.g., proactive audits), detailed above and below.

PRIVACY IMPACT ASSESSMENT (“PIA”): ENHANCE

Ontario proposal: Silent.

344. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance PIAs, by mandating them. This is necessary to implement PbD and demonstrable accountability.
345. This PIAC recommendation is supported by certain key stakeholders, including Canadian privacy commissioners. For example, the October 2019 Joint Resolution by FPT Privacy Commissioners calls for PIAs to be “mandated for all initiatives that involve personal information” (and “for all public funding of such initiatives”). OPCC Annual Report 2018-19 also calls for mandated PIAs.
346. Mandated PIAs would also align with existing and proposed legislative regimes, both Canadian and international. For example, as noted, various EU jurisdictions, pursuant to GDPR, mandate DPIAs. Quebec’s Bill 64 also mandates PIAs.⁴²⁷

RECORD-KEEPING: INTRODUCE

Ontario proposal: Silent.

347. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should mandate record-keeping, defined as the requirement to maintain records to provide evidence of accountability (i.e., compliance with accountability obligations) on request/demand. This is necessary to implement demonstrable accountability.

⁴²⁶ OPCC Annual Report 2019-20.

⁴²⁷ Quebec Bill 64, s. 95. See also: Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business.

348. This PIAC recommendation is supported by certain key stakeholders, including Canadian privacy commissioners. For example, OPCC Annual Report 2018-19 proposes mandated record-keeping on grounds this is necessary to facilitate OPCC’s ability to conduct *proactive* inspections.
349. Mandated record-keeping would also align with existing international legislative regimes (e.g., GDPR).

DATA PROTECTION OFFICER (“DPO”): ENHANCE

Ontario proposal: Silent.

350. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance obligations pertaining to data protection officers, by adopting the GDPR term “Data Protection Officer (DPO)”, including specific requirements/thresholds for appointment (e.g., organizations with X number of employees), and requiring that in organizations handling sensitive or large-scale personal information, the DPO must have “expert knowledge of privacy law and practices”.

SELF-REGULATION MECHANISMS: ENCOURAGE, BUT NOT AS REPLACEMENT FOR LEGISLATED OBLIGATIONS & STRENGTHENED ENFORCEMENT TOOLS

Ontario proposal: Silent.

351. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should “encourage” self-regulatory mechanisms, provides these mechanisms are not viewed or treated as a replacement for legislated obligations and strengthened enforcement tools. Self-regulatory mechanisms are a way to incent compliance, demonstrate accountability, and increase transparency (to the public) and consistency (between organizations). However, we echo OPCC’s warning that: “non-binding schemes for incentivizing adherence with the law would be welcome, but they should not be confused for law” because “they are not legally binding nor enforceable and cannot replace state-made rules adopted in the public interest”.⁴²⁸
352. In particular, PIAC **recommends** that statutorily encouraging self-regulatory mechanisms should include consideration of these GoC Proposals to Modernize PIPEDA:
- Formally recognizing self-regulation by organizations, in the form of industry-led codes of practice (“codes”), technical standards (“standards”), and accreditation/certification schemes (“certification schemes”), “as a means of demonstrating due diligence in regards to compliance with certain provisions”.
 - Empowering privacy commissioners to recognize/validate codes and certification schemes.
 - Granting the relevant Minister (e.g., for PIPEDA, the ISED Minister) regulation-making authority for certification schemes.

RESEARCH CAPACITY: ENHANCE

Ontario proposal: As noted, the Ontario government proposes to expand the mandate for IPC to provide advice/guidance to private organizations, including in the form of research.

353. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance the research capacity of privacy commissioners, by extending the ISED Minister’s authority to ask OPCC to conduct research, consistent with GoC’s Proposals to Modernize PIPEDA.

⁴²⁸ OPCC Annual Report 2018-19.

354. PIAC also welcomes the Minister of Justice’s renewal of the terms and conditions of OPCC’s Contributions Program in 2019-20 for a new 5-year cycle. This program, with an annual budget of \$500,000, funds independent research and related knowledge translation initiatives, for which academic institutions and NFPs (including public interest groups) are eligible.⁴²⁹

ENFORCEMENT TOOLS: ENHANCE

Ontario proposal: As noted, the Ontario government proposes to increase IPC’s power by way of enforcement tools, which could include new powers, specifically order-making power and power to impose penalties (e.g., fines “in severe cases”).

355. As noted, PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance enforcement tools. Privacy enforcement matters more and more in a digital “uber-world” of social media, big data, and AI. Quick and effective mechanisms to enforce privacy legislation, with proportional penalties, are the only way to ensure: proper remedies for individuals; and that private organizations take their privacy obligations seriously, are not financially rewarded for disregarding privacy (aka “legislation does not benefit the offenders”⁴³⁰), do not view “punishment” for non-compliance as an acceptable cost of doing business, and only comply if forced by courts after protracted litigation. This, in turn, is the only way to enhance Canadians’ trust in organizations’ digital practices.
356. This PIAC recommendation is supported by certain key stakeholders, including GoC and Canadian privacy commissioners. For example, the October 2019 Joint Resolution by FPT Privacy Commissioners calls for “(e)ffective independent oversight offices” that “can rely on extensive and appropriate enforcement powers adapted to the digital environment” and for individuals to “have effective means to assert their access and privacy rights and to challenge entities’ compliance with their legislated obligations”. GoC’s Proposals to Modernize PIPEDA and OPCC Annual Report 2018-19 recommend new enforcement mechanisms, with the latter emphasizing that the status quo effectively incentivizes non-compliance, as demonstrated by the Facebook case, and that “(f)or a company like Facebook to dismiss the investigative findings of our Office and think it can decide what legal obligations it will or will not follow is untenable”.
357. Enhanced enforcement tools would also align with existing and proposed legislative regimes, both international (e.g., GDPR) and Canadian (e.g., Quebec’s Bill 64).
358. In addition to the Ontario-proposed enforcement tools, PIAC **recommends** empowering privacy commissioners with the following PIAC-recommended tools.

BINDING RULE-MAKING: INTRODUCE

Ontario proposal: Silent.

359. As noted, PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce *legally binding* “rule-making power” (“binding rule-making power”), defined by OPCC as the power of data protection authorities or other public authorities to issue enforceable codes of conduct, standards, guidance and/or regulation.⁴³¹ We cannot sufficiently emphasize that OPCC’s existing powers do not produce “rules”, “guidance”, or “regulation” that is binding, in the sense that it cannot enforce them directly or indirectly (by going to court).
360. Binding rule-making power would align with most of Canada’s trading partners, including the EU, pursuant to GDPR (see Table in Part 2).

⁴²⁹ OPCC Annual Report 2019-20.

⁴³⁰ September 2020 OPCC Appearance on Quebec’s Bill 64.

⁴³¹ OPCC Annual Report 2019-20.

361. In particular, PIAC **recommends** that legislation should introduce binding guidance (“binding guidance”, “binding subsidiary guidance” or “mandatory guidance”), issued by “a public authority” or privacy commissioners. For privacy commissioners, binding guidance would be developed using their new order-making authority, “through a succession of individual orders”.⁴³² Binding guidance would: “help to clarify how general (obligations) of the Act are to apply in practice” while taking them to “a more concrete level”, thereby providing certainty to individuals and organizations; and could be amended more easily than detailed legislated obligations, as technology and data practices evolve.⁴³³
362. This PIAC recommendation is supported by certain key stakeholders, including Canadian privacy commissioners (e.g., OPCC in its Annual Report 2018-19).

INVESTIGATION & AUDIT: ENHANCE

Ontario proposal: As noted, the Ontario government proposes that IPC could have investigation powers. However, the specified investigation powers appear to be consistent with the current PIPEDA.

363. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance the investigation and audit powers of privacy commissioners, to implement demonstrable accountability, by:
- **Investigation:** Increase discretion on whether to investigate complaints (i.e., not only in defined circumstances), provided this is accompanied by an enhanced private right of action for individuals.
 - **Audit:** Increase flexibility to audit organizations, including power to *proactively* audit privacy compliance where privacy commissioners do not have reasonable grounds to believe there is non-compliance (due to the invisible nature of privacy violations) (aka “proactive inspection without grounds”) and, upon request, provide preliminary opinions on an organization’s proposed privacy practices.
 - **Cooperation:** Facilitate/encourage increased cooperation and information-sharing with other privacy regulators, because: “Multinational firms require multinational responses. It’s therefore essential that countries work together to develop consistent, comprehensive laws and enforcement mechanisms for the protection of personal information.”⁴³⁴
364. This PIAC recommendation is supported by certain stakeholders, including GoC and Canadian privacy commissioners. For example, GoC’s Proposals to Modernize PIPEDA recommend facilitating increase cooperation between Canadian privacy commissioners and their international counterparts. As noted, the October 2019 Joint FPT Privacy Commissioner Resolution calls for power to conduct own-motion investigations and audits. OPCC Annual Report 2018-19 proposes new power to “proactively inspect” and unfettered choice about what complaints to investigate.
365. Enhanced investigation and audit powers would also align with existing international legislative regimes (e.g., GDPR). In particular, the power to proactively audit exists in the UK and several other countries.⁴³⁵
366. Further, PIAC **recommends** that legislation should enhance joint privacy enforcement by Canadian *non-privacy* regulators (aka “regulators with different mandates”), by authorizing information-sharing, to enhance the collective privacy (and other) protection of Canadians. OPCC Annual Report 2019-20 notes that in the past year, OPCC has entered into more joint investigations with PT privacy commissioners than ever before, however “under the current legal framework, we may collaborate with international partners in circumstances where we would not be able to do with Canadian (non-privacy) regulators” (e.g., Competition Bureau, outside CASL-related matters).

⁴³² OPCC Annual Report 2018-19.

⁴³³ OPCC Annual Report 2018-19.

⁴³⁴ Privacy in Canada: A Public Interest Perspective – Address to the Rile Conference on Privacy and Bill C-54.

⁴³⁵ OPCC Annual Report 2018-19.

FINANCIAL PENALTIES: ENHANCE

Ontario proposal: As noted, the Ontario government proposes that IPC could have new powers, specifically power to impose penalties (e.g., fines “in severe cases”). It is uncertain whether “fines” means administrative fines (i.e., AMPs) and/or penal fines.

(Note: while penal fines are generally imposed by courts, they can be imposed by privacy commissioners, as demonstrated by Quebec Bill 64 [see details below].)

367. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance financial penalties. A 2016 public opinion survey found more Canadians are willing to do business with organizations if they face strict financial penalties for misusing personal information.⁴³⁶
368. This PIAC recommendation is supported by certain key stakeholders, including Canadian privacy commissioners. For example, the October 2019 Joint Resolution by FPT Privacy Commissioners calls for all governments to put in place enforcement powers, including legislating powers to impose penalties, and OPCC Annual Report 2018-19 recommends new enforcement mechanisms, including OPCC power to impose penalties under PIPEDA.
369. In particular, PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance financial penalties in the following ways.

FINES (IMPOSED BY COURTS): EXTEND & INCREASE

370. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should extend the existing regime for fines (imposed by courts) to all key statutory provisions of the Act (e.g., consent requirements and data safeguards) and substantially increase the range of fines, with a scheme for mitigating/aggravating factors.
371. This PIAC recommendation is supported by certain stakeholders, including GoC. For example, GoC’s Proposals to Modernize PIPEDA include extending the existing regime for fines to other key provisions of the Act⁴³⁷ (e.g., consent requirements and data safeguards) and substantially increasing the range of fines together with a scheme for mitigating/aggravating factors.
372. Extending the regime for, and range of, fines would also align with proposed Canadian legislative regimes. For example, Quebec’s Bill 64 provides for penal fines, imposed by CAI, of up to \$25 million or 4% of worldwide turnover, whichever is greater, with a minimum fine of \$15,000 (substantially increased from the current maximum penalty of \$50,000 under the Private Sector Act).⁴³⁸ This “would make the Private Sector Act the most punitive privacy law in the (sic) Canada”, with a potential fine exceeding those available under the Competition Act and CASL.⁴³⁹

⁴³⁶ PIAC 2017 Final Submission to ETHI Review of PIPEDA, footnote 9 (citing “2016 Survey of Canadians on Privacy: Final Report (2016)”, OPCC, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12, Figure 19.

⁴³⁷ PIPEDA Consultation Paper (“Under PIPEDA as currently drafted, there are two categories of offence: an offence punishable on summary conviction and liable to a fine not exceeding \$10,000 (per offence); an indictable offence and liable to a fine not exceeding \$100,000 — (maximum of \$100,000 per offence). These categories of offences are distinguished based on the severity of the contravention. Typically, summary offences are less serious than indictable offences. The Attorney General of Canada has the discretionary power to qualify the contravention as either type of offence depending on the nature of the contravention. Fines are applied by the Courts.”)

⁴³⁸ Quebec Bill 64, s. 151. See also: Torys: Ontario Enters the Private Sector Privacy Realm; Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business; Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR; Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

⁴³⁹ Quebec to Introduce the Most Punitive Privacy Laws in Canada.

ADMINISTRATIVE MONETARY PENALTIES (“AMPs”) (IMPOSED BY PRIVACY COMMISSIONERS): INTRODUCE – SEE BELOW

373. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce AMPs, together with binding orders (see details below).

BINDING ORDERS & AMPs: INTRODUCE

Ontario proposal: As noted, the Ontario government proposes that IPC could have new powers, specifically order-making power and, possibly, AMP power.

374. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce:
- **Order-making powers:** defined by OPCC as the power of data protection authorities to back findings with orders for particular remedies⁴⁴⁰ (i.e., “ombudsman with a stick”), including cessation and records preservation orders, which should be subject to judicial review; *together with*
 - **Administrative fines/AMPs:** that privacy commissioners can impose for violations identified following an investigation, which should be sizable and subject to commissioner discretion and flexibility to determine when to impose them.

We believe these combined powers would ensure that organizations comply expeditiously with privacy protections and “change the dynamic of (privacy commissioners’) discussions with companies during investigations, leading to quicker resolutions for Canadians”.⁴⁴¹ In particular, order-making power would serve as an important deterrent, regardless of how frequently it is used, thereby leading to additional compliance, and this tangible benefit outweighs the alleged risks (e.g., negative reaction by businesses, increased adversarial tensions, litigiousness, and added cost/complexity for privacy commissioners and organizations).

375. This PIAC recommendation is supported by certain key stakeholders, including GoC and Canadian privacy commissioners. For example, GoC’s Proposals to Modernize PIPEDA include order-making power (including cessation and records preservation orders). The October 2019 Joint Resolution by FPT Privacy Commissioners calls for all governments to legislate powers to make orders and impose AMPs. OPCC Annual Report 2018-19 recommends granting OPCC power to issue binding orders and AMPs under PIPEDA, because recent cases “attest to the failings of accountability and safeguards in current business models”. In particular: “(t)he most prominent investigations we conducted under PIPEDA in 2018-2019 were about the Facebook/Cambridge Analytica scandal and the Equifax data breach”; the former “found that Facebook had committed serious contraventions of Canadian privacy laws” but “ended with the social media giant’s deeply disappointing decision not to implement recommendations aimed at correcting serious privacy deficiencies”; and “(f)or these reasons, our Office announced its intention to apply to the Federal Court to seek a binding order to force the company to take action to correct its privacy practices”.
376. Order-making and AMP powers would also align with existing and proposed legislative regimes, both international and Canadian. For example, order-making and AMP powers (subject to judicial review) are held by privacy commissioners in most of Canada’s trading partners (e.g., EU and US – see Table in Part 2) and by certain Canadian regulators (privacy and non-privacy – see below), who “report that these enforcement tools have led to much more cooperation from companies” and “(w)hen the regulator finds a violation, companies are more willing to correct deficiencies, without long delays”.⁴⁴² Canadian regulators with AMPs tend to be cautious in imposing them, first resorting to other tools (e.g., warnings, compliance

⁴⁴⁰ OPCC Annual Report 2019-20.

⁴⁴¹ OPCC Annual Report 2018-19.

⁴⁴² OPCC Annual Report 2018-19.

letters, “naming and shaming”, and voluntary undertakings) and, finally, notices of violation with AMPs that are tailored on a principled basis to the gravity of the violation (amongst other factors).⁴⁴³

377. PT privacy commissioners with order-making power include IPC⁴⁴⁴ and the AB, BC, and QC Commissioners pursuant to “substantially similar” PT general private sector privacy legislation. In 2015, the Ontario Ministry of the Attorney General noted that “AMP systems are becoming widely accepted as the modern approach to regulation in Ontario, across Canada and around the world”.⁴⁴⁵ Today, AMP powers are held by certain Canadian regulators, both privacy (e.g., IPC, which as of August 2020 “does not yet have firsthand experience in issuing administrative penalties”⁴⁴⁶ but has the power to do so under PHIA, pursuant to March 2020 revisions) and non-privacy (e.g., CRTC pursuant to the *Telecommunications Act*). Quebec’s Bill 64 proposes significant AMPs, of up to \$10 million or 2% of worldwide turnover, whichever is greater (subject to an internal review process and judicial review).⁴⁴⁷
378. For clarity, PIAC **opposes** “circumscribed” order-making power, for the same reasons it is opposed by OPCC: it “is not only inefficient, but ineffective” and “would cause delay and encourage limited compliance”.⁴⁴⁸ In particular, we oppose requiring privacy commissioners to refer matters of concern to the relevant AG for investigation (“AG review”), as recommended in the Digital Charter and GoC’s Proposals to Modernize PIPEDA. An AG review, which would mean that when a privacy commissioner investigation results in a finding of non-compliance, the commissioner must first convince the AG to further investigate and bring an action in court, would be “very inefficient, given it would seriously delay the enjoyment of rights by individuals to several years after they have filed a complaint. Justice delayed is justice denied.”⁴⁴⁹
379. Further, PIAC **recommends** that privacy commissioners (federal or Ontario) with AMPs should follow the best practice of regulators with this power to regularly reach out to affected organization sectors and their associations to educate them on regulators’ expectations, to avoid any element of unfair surprise.

PRIVATE RIGHT OF ACTION & STATUTORY DAMAGES: ENHANCE

Ontario proposal: Silent.

380. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should enhance the existing limited private right of action. We believe this is essential in a (new) right-based model, would provide an effective tool for fulfilling (new) legislative objectives, and would recognize that privacy commissioners with limited resources cannot investigate every alleged statutory breach. “In an age in which privacy, technology, and law collide more than ever, it stands to be an adjudicative mechanism of ever-increasing importance.”⁴⁵⁰
381. In particular, PIAC **recommends** that legislation should enhance the private right of action in ways that include:
- **Delete limits:** Remove the statutory pre-requisite for privacy commissioner involvement and permit usage for privacy complaints beyond data security breaches.
 - **Enable statutory damages:** Empower courts to order statutory damages for certain violations.

⁴⁴³ See e.g., the “factors for penalty” in CASL, s. 20(3).

⁴⁴⁴ Currently, IPC has order-making power under FIPPA and MFIPPA (only for access) and PHIPA (for access and privacy); Ontario consultation paper, p. 7. Under FIPPA and MFIPPA, its power to issue a binding order is subject to judicial review but not to appeal: IPC: Freedom of Information and Privacy Manual – Appeals and Compliance.

⁴⁴⁵ Exploring an Online Administrative Monetary Penalty System for Infractions of Provincial Statutes and Municipal By-Laws in Ontario.

⁴⁴⁶ Submission of the Information and Privacy Commissioner of Ontario to the Special Committee to Review the Personal Information Protection Act (BC) (citing Bill 188, *Economic and Fiscal Update Act, 2020*, Sched. 6, and noting that regulations pertaining to AMPs have not yet been drafted).

⁴⁴⁷ Quebec Bill 64, s. 150. See also: Torys: Ontario Enters the Private Sector Privacy Realm; Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

⁴⁴⁸ OPCC Annual Report 2019-20; Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business.

⁴⁴⁹ OPCC Annual Report 2018-19.

⁴⁵⁰ Damages under PIPEDA: A Purposive Approach and a New High Water Mark.

- **Prescribe statutory damage range:** Prescribe a range of statutory damage awards, with a significant maximum (because personal information is valuable, and low amounts merely constitute a “cost of doing business” from the perspective of non-compliant organizations with deep pockets).

These enhancements would facilitate access to justice by providing individuals with the option to select set damages without needing to prove actual damages, simplify the hearing process by streamlining damages, and maintain consistency, predictability, and fairness in court decisions on entitlement to and quantification of damages.

382. These PIAC recommendations are supported by certain key stakeholders, including GoC and Canadian privacy commissioners. For example, OPCC Annual Report 2018-19 recommends providing individuals with an enhanced private right of action under PIPEDA. GoC’s Proposals to Modernize PIPEDA include empowering the Federal Court to order statutory damages for certain violations and prescribing a range of statutory damage awards.
383. An enhanced private right of action would also align with:
- international legislative regimes, both existing (e.g., GDPR – see Table in Part 2) and proposed (e.g., the proposed NYPA, which provides individuals with a right to sue businesses directly over privacy violations).
 - proposed Canadian legislative regimes, notably Quebec’s Bill 64, which introduces a civil cause of action for statutory damages based on violation of a right granted in the Private Sector Act or a right relating to privacy protection in the Civil Code of Québec and, where the violation is intentional or results from gross fault, punitive damages of at least \$1,000.⁴⁵¹
384. PIAC emphasizes that it is essential for any private right of action to be part of a broader, strengthened enforcement toolkit. We are sceptical about the effectiveness of a private right of action, on a stand-alone basis, because it shifts the burden of enforcement to individuals, who will rarely have the willingness, ability, or resources to self-fund a lawsuit (absent a funding program, such as exists for Charter challenges under the Court Challenges Program [“CCP”]⁴⁵²). For this reason, we **recommend** that a fund should be established, perhaps as a new component of the CCP, to assist individual complainants in exercising their privacy rights and enforcing the law via court actions, where appropriate.
385. Further, PIAC **recommends** that legislation should permit usage for privacy complaints beyond data security breaches and expressly permit privacy class actions, consistent with GDPR. As Justice Glustein observed in October 2019, in *Haikola v. Personal Insurance Co.*, at para 88: “If systemic PIPEDA privacy breaches are not rectified by a class procedure, it is not clear what incentive large insurers and others will have to avoid overcollection of information” at least unless/until OPCC is granted enhanced powers to enforce compliance through strong regulatory penalties. We note that the Quebec Bill 64 private right of action, according to Eloïse Gratton, co-lead of the national privacy and data protection practice at Borden Gervais LLP, “may translate in Quebec becoming an even friendlier jurisdiction for privacy class actions”.⁴⁵³

SCALABLE ENFORCEMENT: INTRODUCE, FOR MITIGATING/AGGRAVATING FACTORS

Ontario proposal: Silent. However, as noted, the Ontario government proposes scalable *compliance*, based on the size of the organization.

⁴⁵¹ Quebec Bill 64, s. 152. See also: Torys: Ontario Enters the Private Sector Privacy Realm (noting currently, “it is only possible to obtain punitive damages for a privacy breach under the Québec Charter where the breach is both unlawful and intentional”); Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business; Canada: Bill 64: Modernizing Québec’s Privacy Regime; Quebec to Introduce the Most Punitive Privacy Laws in Canada; Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime.

⁴⁵² DCH: Court Challenges Program.

⁴⁵³ Quebec Plans Ambitious Overhaul of its Privacy Law (citing Gratton).

386. PIAC **recommends** that general private sector privacy statutes (PIPEDA or Ontario) should introduce scalable enforcement that pertains to all covered organizations. For example, as noted, PIAC recommends that fines should be increased together with a scheme for mitigating/aggravating factors.

CONCLUSION: SUMMARY OF PIAC RECOMMENDATIONS

387. In conclusion, PIAC makes the following recommendations:

- Bolster privacy protections in Ontario’s private sector, by strengthening the federal PIPEDA and introducing provincial employment privacy legislation. Comprehensive Canadian privacy law reform is urgently needed, driven by the digital privacy gap and adequacy gaps with GDPR.
- In particular, GDPR-ize general private sector privacy legislation – PIPEDA or a new Ontario statute – by enhancing its scope, privacy protections (both organization obligations and individual rights), and compliance/enforcement. To reiterate Canadian Privacy Commissioner Therrien: “Canadians want to enjoy the benefits of digital technologies, but they want to do it safely. Legislation should recognize and protect their freedom to live and develop independently as persons, away from the watchful eye and unconscious influence of a surveillance state or commercial enterprises, while still participating voluntarily and safely in the day-to-day activities of a modern society.”⁴⁵⁴

388. We would welcome the opportunity to elaborate on our proposals and the significant interests of Canadian citizen-consumers in strong privacy protections at any subsequent stage(s) of the Ontario Privacy Consultation.

389. All of which is respectfully submitted.

⁴⁵⁴ OPCC News release: Commissioner’s Annual Report Sets out Blueprint for How to Modernize Canadian Privacy Laws.

APPENDIX: BIBLIOGRAPHY

GOVERNMENT SOURCES (CANADIAN)

Governments (Federal & Provincial/Territorial ["FPT"])

- "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians", ISED, 2019, online: [https://www.ic.gc.ca/eic/site/062.nsf/vwapi/Digitalcharter_Report_EN.pdf/\\$file/Digitalcharter_Report_EN.pdf](https://www.ic.gc.ca/eic/site/062.nsf/vwapi/Digitalcharter_Report_EN.pdf/$file/Digitalcharter_Report_EN.pdf) ("Digital Charter"). See also "Canada's Digital Charter: Trust in a Digital World", ISED, online: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html (last modified September 10, 2020; accessed September 25, 2020) ("Canada's Digital Charter: Trust in a Digital World").
- "Canada's Federal Privacy Laws: Background Paper", Publication No. 2007-44-E, Library of Parliament (Miguel Bernal-Castillero, Economics, Resources and International Affairs Division), October 1, 2013, online: https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/200744E ("Canada's Federal Privacy Laws: Background Paper").
- "Consultation: Strengthening Privacy Protections in Ontario", Ontario Ministry of Government and Consumer Services ("Ontario MGCS"), August, 13, 2020 (last modified September 22, 2020; accessed September 23, 2020), online: <https://www.ontario.ca/page/consultation-strengthening-privacy-protections-ontario> ("Ontario government consultation website").
- "Court Challenges Program", Department of Canadian Heritage, online: <https://www.canada.ca/en/canadian-heritage/services/funding/court-challenges-program.html> (last revised June 19, 2020; accessed October 6, 2020) ("DCH: Court Challenges Program").
- "Declaration of PHIPA as Substantially Similar to PIPEDA", Ontario Ministry of Health and Long-Term Care, online: http://www.health.gov.on.ca/english/providers/project/priv_legislation/hipha_pipeda_qa.html (accessed August 14, 2020) ("Declaration of PHIPA as Substantially Similar to PIPEDA").
- "Directive on Privacy Impact Assessment", Treasury Board of Canada Secretariat, April 1, 2010, online: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308> ("TBS Directive on Privacy Impact Assessment").
- "Exploring an Online Administrative Monetary Penalty System for Infractions of Provincial Statutes and Municipal By-Laws in Ontario", Ontario Ministry of the Attorney General, March 3, 2015, online: https://www.attorney-general.jus.gov.on.ca/english/POA%20ConsultationPaper%20Final_ENG.html ("Exploring an Online Administrative Monetary Penalty System for Infractions of Provincial Statutes and Municipal By-Laws in Ontario").
- "Interim Directive on Privacy Impact Assessment", Treasury Board Secretariat, March 13, 2020, online: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308§ion=html> (last modified June 18, 2020; accessed July 31, 2020) ("Interim Directive on Privacy Impact Assessment").
- Legislative Assembly of British Columbia, Parliamentary Committees, Special Committee to Review the Personal Information Protection Act, online: <https://www.leg.bc.ca/parliamentary-business/committees/41stParliament-5thSession-pipa/> ("Legislative Assembly of British Columbia, Parliamentary Committees, Special Committee to Review the Personal Information Protection Act").
- "Minister Bains announces Canada's Digital Charter", ISED, May 21, 2019, online: <https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/minister-bains-announces-canadas-digital-charter.html> ("Minister Bains announces Canada's Digital Charter").
- "Minister of Innovation, Science and Industry Mandate Letter", Office of the Prime Minister, December 13, 2019, online: <https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-innovation-science-and-industry-mandate-letter> ("December 2019 ISED Minister Mandate Letter").
- "Modernizing Canada's Privacy Act", Department of Justice, online: <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html> (last modified June 5, 2020; accessed September 25, 2020) ("Modernizing Canada's Privacy Act").
- "News Release: Ontario Launches Consultations to Strengthen Privacy Protections of Personal Data", Ontario Government, August 13, 2020, online: <https://news.ontario.ca/en/release/57985/ontario-launches-consultations-to-strengthen-privacy-protections-of-personal-data> ("News Release: Ontario Launches Consultations to Strengthen Privacy Protections of Personal Data" or "Ontario government news release").
- "Ontario Private Sector Privacy Reform: Improving Private Sector Privacy for Ontarians in a Digital Age – Discussion Paper", Ontario government, August 13, 2020, online: <https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45105> ("Ontario government discussion paper" or "Ontario government consultation paper").

- “Privacy and Digital Government Services: Report of the Standing Committee on Access to Information, Privacy and Ethics”, ETHI, June 2019, online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10583346/ethirp19/ethirp19-e.pdf> (“ETHI Report”).
- “Privacy Impact Assessment”, Statistics Canada, online: <https://www.statcan.gc.ca/eng/about/pia/pia> (accessed June 9, 2020) (“Statistics Canada, Privacy Impact Assessment”).
- “Public Consultation - Reforming Privacy in Ontario's Private Sector”, Ontario’s Regulatory Registry, online: <https://www.ontariocanada.com/registry/view.do?language=en&postingId=33967> (“Ontario’s Regulatory Registry”).
- “Sixth Update Report on Developments in Data Protection Law in Canada: Report to the European Commission December 2019”, ISED, March 10, 2020, online: https://www.ic.gc.ca/eic/site/113.nsf/eng/h_07668.html (“Sixth Update Report on Developments in Data Protection Law in Canada: Report to the European Commission December 2019”).
- “Strengthening Privacy for the Digital Age”, ISED, May 21, 2019, online: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html (“Strengthening Privacy for the Digital Age” or “GoC’s Proposals to Modernize PIPEDA”).
- “The European Union’s General Data Protection Regulation”, Government of Canada, Trade Commissioner Services, online: <https://www.tradecommissioner.gc.ca/guides/gdpr-eu-rgpd.aspx> (last modified November 19, 2020; accessed September 28, 2020) (“Trade Commissioner: The European Union’s General Data Protection Regulation”).

Courts

- Affidavit of Sean McDonald*, Court File No. 211/19, May 28, 2019, in *CCLA v. Waterfront Toronto, et al.* (“Affidavit of Sean McDonald in *CCLA v. Waterfront Toronto, et al.*”).
- Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, online: <http://www.canlii.org/en/ca/fca/doc/2006/2006fca157/2006fca157.html> (“*Canada [Information Commissioner] v. Canada [Transportation Accident Investigation and Safety Board]*”).
- Haikola v. The Personal Insurance Company*, 2019 ONSC 5982 (CanLII), online: <http://canlii.ca/t/j2w6h> (retrieved October 12, 2020) (“*Haikola v. The Personal Insurance Company*”).

Regulators (e.g., Privacy Commissioners [FPT] and CRTIC)

- “A Data Privacy Day Conversation with Canada’s Privacy Commissioner”, Privacy Commissioner of Canada (Daniel Therrien), Remarks at the University of Ottawa’s Centre for Law, Technology and Society, January 28, 2020, online: https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200128/ (“A Data Privacy Day Conversation with Canada’s Privacy Commissioner”).
- “A Guide for Individuals Protecting Your Privacy”, OPC, online: https://www.priv.gc.ca/en/about-the-opc/publications/guide_ind/ (accessed 21 May and 17 June 2020) (“OPC A Guide for Individuals Protecting Your Privacy”).
- “Appearance before the Committee on Institutions of the National Assembly of Quebec regarding Bill 64, An Act to Modernize Legislation Provisions as Regards the Protection of Personal Information”, OPCC, September 24, 2020, online: https://priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200924/ (“September 2020 OPCC Appearance on Quebec’s Bill 64”).
- “Commercial Activity”, OPCC, January 2017, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/ (“OPCC: Commercial Activity”).
- “Consultation on the OPCC’s Proposals for Ensuring Appropriate Regulation of Artificial Intelligence”, OPCC, January 28, 2020, online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/#fn6-rf (“Consultation on the OPCC’s Proposals for Ensuring Appropriate Regulation of Artificial Intelligence”).
- “De-Identification Guidelines for Structured Data”, IPC, June 8, 2016, online: <https://www.ipc.on.ca/resource/de-identification-guidelines-for-structured-data/> (“IPC: De-Identification Guidelines for Structured Data”).
- “Effective Privacy and Access to Information Legislation in a Data Driven Society: Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners”, October 1-2, 2019, online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_191001/ (“October 2019 Joint Resolution by FPT Privacy Commissioners”).
- “Enforcement of PIPEDA”, OPCC, online: <https://www.priv.gc.ca/biens-assets/compliance-framework/en/index#&ui-state=dialog> (last modified April 20, 2017, accessed October 6, 2020) (“OPCC: Enforcement of PIPEDA”).
- “Expectations: OPC’s Guide to the Privacy Impact Assessment Process”, OPC, revised March 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/ (“Expectations: OPC’s guide to the”).

privacy impact assessment process” or “Expectations: OPC’s Guide to the Privacy Impact Assessment Process, March 2020”).

- “Freedom of Information and Privacy Manual – Appeals and Compliance”, IPC May 23, 2019, online: <https://www.ontario.ca/document/freedom-information-and-privacy-manual/appeals-and-compliance> (“IPC: Freedom of Information and Privacy Manual – Appeals and Compliance”).
- “Frequently Asked Questions for Online Consent”, OPCC, May 2014, online: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_oc_201405_faq/ (“OPCC: FAQ for Online Consent”).
- “Guidelines for Obtaining Meaningful Consent”, OPCC and the Offices of the Information and Privacy Commissioner of Alberta (“OIPC-AB”) and British Columbia (“OIPC-BC”), May 2018, online: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ (“Guidelines for Obtaining Meaningful Consent”).
- “How PIPEDA Applies to Charitable and Non-profit Organizations”, OPCC, revised June 2019, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_19/ (“OPCC: How PIPEDA Applies to Charitable and Non-profit Organizations”).
- “How to Apply for a Federal Court Hearing Under PIPEDA”, OPCC, September 2016, online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/federal-court-applications-under-pipeda/> (“OPCC: How to Apply for a Federal Court Hearing Under PIPEDA”).
- “News Release: Commissioner’s Annual Report: Pandemic Raises Privacy Concerns Highlighting Urgency of Law Reform”, OPCC, October 8, 2020, online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201008/ (“News Release: Commissioner’s Annual Report: Pandemic Raises Privacy Concerns Highlighting Urgency of Law Reform”).
- “News Release: Commissioner’s Annual Report Sets Out Blueprint for How to Modernize Canadian Privacy Laws”, OPCC, December 10, 2019, online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_191210/ (“OPCC News Release: Commissioner’s Annual Report Sets Out Blueprint for How to Modernize Canadian Privacy Laws”).
- “Personal Information”, OPCC, October 2013, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/ (“OPCC: Personal Information”).
- “PIPEDA Fair Information Principle 1 – Accountability”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/ (“PIPEDA Fair Information Principle 1 – Accountability”);
- “PIPEDA Fair Information Principle 2 – Identifying Purposes”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_purposes/ (“PIPEDA Fair Information Principle 2 – Identifying Purposes”).
- “PIPEDA Fair Information Principle 3 – Consent”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/ (“PIPEDA Fair Information Principle 3 – Consent”).
- “PIPEDA Fair Information Principle 4 – Limiting Collection”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_collection/ (“PIPEDA Fair Information Principle 4 – Limiting Collection”).
- “PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/ (“PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention”).
- “PIPEDA Fair Information Principle 6 – Accuracy”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accuracy/ (“PIPEDA Fair Information Principle 6 – Accuracy”).
- “PIPEDA Fair Information Principle 7 – Safeguards”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/ (“PIPEDA Fair Information Principle 7 – Safeguards”).
- “PIPEDA Fair Information Principle 8 – Openness”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_openness/ (“PIPEDA Fair Information Principle 8 – Openness”).
- “PIPEDA Fair Information Principle 9 – Individual Access”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_access/ (“PIPEDA Fair Information Principle 9 – Individual Access”).

- “PIPEDA Fair Information Principle 10 – Challenging Compliance”, OPCC, reviewed August 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_compliance/ (“PIPEDA Fair Information Principle 10 – Challenging Compliance”).
- “Privacy in a Pandemic: 2019-2020 Annual Report to Parliament on the Privacy Act and Personal Information Protection Electronic Documents Act”, OPCC, October 8, 2020, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201920/ar_201920/ (“OPCC Annual Report 2019-20”).
- “Privacy Law Reform – A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy: 2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act”, OPCC, December 10, 2019, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/ (“OPCC Annual Report 2018-19”).
- “Provincial Laws that May Apply Instead of PIPEDA”, OPCC, reviewed May 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/ (“OPCC: Provincial Laws that May Apply Instead of PIPEDA”).
- “Remarks by Privacy Commissioner of Canada regarding his 2019-2020 Annual Report to Parliament”, OPCC (Privacy Commissioner Daniel Therrien), October 8, 2020, online: https://www.priv.gc.ca/en/opc-news/speeches/2020/sd_20201008/ (“Remarks by Privacy Commissioner of Canada regarding his 2019-2020 Annual Report to Parliament”).
- “Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps”, Joint OPCC and Alberta and British Columbia Privacy Commissioner Guidance, October 2012, online: https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/gd_app_201210/ (“Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps”).
- “Submission of the Information and Privacy Commissioner of Ontario to the Special Committee to Review the Personal Information Protection Act (British Columbia)”, Ontario Privacy Commissioner Patricia Kosseim, August 2020, online: <https://www.ipc.on.ca/wp-content/uploads/2020/08/2020-08-14-submission-to-bc-special-committee.pdf> (“Submission of the Information and Privacy Commissioner of Ontario to the Special Committee to Review the Personal Information Protection Act (BC)”).
- “The Case for Reforming the Personal Information Protection and Electronic Documents Act”, OPCC, May 2013, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/#fn3-rf (“The Case for Reforming the Personal Information Protection and Electronic Documents Act”).
- “The Personal Information Protection and Electronic Documents Act (PIPEDA)”, OPCC, online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/> (last modified September 4, 2019; accessed September 21, 2020) (“OPCC: PIPEDA”).
- “What you need to know about mandatory reporting of breaches of security safeguards”, OPCC, October 2018, online: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/ (“OPCC: What You Need to Know About Mandatory Reporting of Breaches of Security Safeguards”).

OTHER SOURCES (CANADIAN & INTERNATIONAL)

- “2020 Consultation on the Personal Information Protection Act, Submission by Retail Council of Canada- Special Committee to Review the Personal Information Protection Act”, Retail Council of Canada (“RCC”), August 14, 2020), online: https://www.leg.bc.ca/content/CommitteeDocuments/41st-parliament/5th-session/pipa/submissions/1042-12396_Retail-Council-Canada_Submission.pdf (“Submission by Retail Council of Canada to Special Committee to Review the BC Personal Information Protection Act”).
- “A European Strategy for Data”, European Commission, online: <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy> (last revised September 30, 2020; accessed October 4, 2020) (“EC: A European Strategy for Data”).
- “A European Strategy for Data: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2020/66 final”, European Commission, February 19, 2020, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066> (“European Data Strategy”).
- “A New Privacy Law for Ontario? Towards a ‘Made-in-Ontario’ Response to Global Developments”, Fasken Martineau DuMoulin LLP, September 3, 2020, online: <https://www.fasken.com/en/knowledge/2020/09/2-new-privacy-law-ontario/> (“A New Privacy Law for Ontario?”)

- “A ‘Privacy First’ Canadian Public Policy Approach to Digital Contact Tracing (“DCTT”) Related to COVID-19 & Future Pandemics”, PIAC, filed with CRTC on September 9, 2020 as Appendix 1 of PIAC’s Telecommunications Part 1 Application requesting CRTC oversight of potential linkages between IP addresses generated by use of Health Canada’s “COVID Alert” app (as well as similar uses of IP addresses and additionally, mobile phone numbers, by the ‘ABTraceTogether” app in Alberta) and telecommunications subscriber information, online: <https://www.piac.ca/wp-content/uploads/2020/09/Appendix-1-PIAC-Position-Paper-Covid19-DCTT-FINAL-9-Sept-2020.pdf> (“PIAC Position Paper on DCTT and Privacy”).
- “A Private Sector Privacy Law for Ontario: A Step in the Right Direction?”, PIAC, October 1, 2020, online: <https://www.piac.ca/a-private-sector-privacy-law-for-ontario-a-step-in-the-right-direction/> (“A Private Sector Privacy Law for Ontario: A Step in the Right Direction?”)
- “A Typology of Privacy”, B. Koops et al, Penn Law: Legal Scholarship Repository, 2017, online: <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1938&context=jil> (“A Typology of Privacy”).
- “Adequacy Decisions: How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection”, European Union, online: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed September 28, 2020) (“Adequacy Decisions: How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection”).
- “Algorithmic bias”, Wikipedia, online: https://en.wikipedia.org/wiki/Algorithmic_bias (accessed October 14, 2020) (“Wikipedia: Algorithmic bias”).
- “Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business”, McCarthy Tetrault LLP, June 19, 2020, online: <https://www.mccarthy.ca/en/insights/blogs/techlex/bill-64-overhaul-quebecs-privacy-law-regime-implications-business> (“Bill 64: An Overhaul of Quebec’s Privacy Law Regime – Implications for Business”).
- “Bridging the Gaps: a Path Forward to Federal Privacy Legislation”, Report, Brookings (C. F. Kerry et al), June 3, 2020, online: https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf (“Brookings Report, Bridging the Gaps: a Path Forward to Federal Privacy Legislation”).
- “Canada: An Employer’s Guide to Privacy in the Workplace”, Mondaq (Dentons), August 16, 2018, online: <https://www.mondaq.com/canada/privacy-protection/728526/an-employer39s-guide-to-privacy-in-the-workplace> (“Canada: An Employer’s Guide to Privacy in the Workplace”).
- “Canada: Bill 64: Modernizing Quebec’s Privacy Regime”, Mondaq (McMillan LLP), August 6, 2020, online: <https://www.mondaq.com/canada/privacy-protection/973602/bill-64-modernizing-qubec39s-privacy-regime> (“Canada: Bill 64: Modernizing Quebec’s Privacy Regime”).
- “Canada: Cybersecurity Comparative Guide”, Mondaq (INQ Data Law, Carole Piovesan), July 7, 2020 (“Canada: Cybersecurity Comparative Guide”).
- “Canada: Implementing Privacy By Design”, Mondaq (Miller Thomson LLP, David Krebs), November 12, 2018, online: <https://www.mondaq.com/canada/Privacy/753378/Implementing-Privacy-By-Design> (“Canada: Implementing Privacy By Design”).
- “Canada: Modernizing Federal Privacy Laws: Suggested Approaches of the Federal Government and the OPC”, Mondaq (S Pinsky & P Brown), June 8, 2020, online: <https://www.mondaq.com/canada/privacy-protection/949554/modernizing-federal-privacy-laws-suggested-approaches-of-the-federal-government-and-the-opc?signup=true> (“Canada: Modernizing Federal Privacy Laws: Suggested Approaches of The Federal Government and the OPC”).
- “Canada: Ontario Tries Again – Provincial Government Launches Consultation on Strengthening Provincial Privacy Laws”, Mondaq (Cassels), August 18, 2020, online: <https://www.mondaq.com/canada/privacy-protection/977144/ontario-tries-again-provincial-government-launches-consultation-on-strengthening-provincial-privacy-laws> (“Canada: Ontario Tries Again – Provincial Government Launches Consultation on Strengthening Provincial Privacy Laws”).
- “Canada: Putting a Dollar Figure on Breach of Privacy in Canada”, Mondaq (Fogler, Rubinoff LLP), January 26, 2017, online: <https://www.mondaq.com/canada/privacy-protection/563430/putting-a-dollar-figure-on-breach-of-privacy-in-canada> (“Canada: Putting a Dollar Figure on Breach of Privacy in Canada”).
- “Canada: Special Committee Begins Consultations On Changes To BC’s Personal Information Protection Act”, Mondaq (McCarthy Tetrault LLP), May 13, 2020, online: <https://www.mondaq.com/canada/privacy-protection/933052/special-committee-begins-consultations-on-changes-to-bc39s-personal-information-protection-act> (“Canada: Special Committee Begins Consultations On Changes To BC’s Personal Information Protection Act”).
- “Canada: The Growing Importance Of Privacy Compliance In Transactions”, Mondaq (Miller Thomson), August 4, 2017, online: <https://www.mondaq.com/canada/privacy-protection/616776/the-growing-importance-of-privacy-compliance-in-transactions> (“Canada: The Growing Importance Of Privacy Compliance In Transactions”).

- “Canada: Trust Basics”, Mondaq (Norton Rose Fulbright), December 23, 2016, online: <https://www.mondaq.com/canada/trusts/555766/trust-basics> (“Canada: Trust Basics”).
- “Canada: Understanding the Differences between GDPR, CCPA, and PIPEDA – A Guide for Canadian Businesses”, Mondaq (Siskinds), January 14, 2020, online: <https://www.mondaq.com/canada/data-protection/883334/understanding-the-differences-between-gdpr-ccpa-and-pipeda-a-guide-for-canadian-businesses> (“Canada: Understanding the Differences between GDPR, CCPA, and PIPEDA”).
- “Canada Can Do More to Protect Our Children Online”, Boys & Girls Clubs of Canada (Owen Charters), February 7, 2017, online: <https://www.bgccan.com/en/WhatsNew/NewsListings/Pages/Canada-Can-Do-More-To-Protect-Our-Children-Online.aspx> (“Canada Can Do More to Protect Our Children Online”).
- “Canadian Anonymization Network: FAQ”, Canadian Anonymization Network (“Canon”), January 15, 2020, online: <https://deidentify.ca/wp-content/uploads/2020/01/CANON-FAQ.pdf> (“Canadian Anonymization Network: FAQ”).
- “Chapter 1: The Rapid Evolution of Data Protection Laws”, White & Case LLP, in ICLG’s *The International Comparative Guide to Data Protection 2018*, 5th edition (“Chapter 1: The Rapid Evolution of Data Protection Laws, in *The International Comparative Legal Guide to Data Protection 2018*”).
- “Chapter 5: Key Definitions – Unlocking the EU General Data Protection Regulation”, White & Case, April 5, 2019, online: <https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation> (“Chapter 5: Key Definitions – Unlocking the EU General Data Protection Regulation”).
- “Chapter 7: Canada”, Osler, Hoskin & Harcourt LLP, in ICLG’s *The International Comparative Guide to Data Protection 2018*, 5th edition, online: <https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf> (“Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*”).
- “Chapter 7: Legal Basis for Processing – Unlocking the EU General Data Protection Regulation”, White & Case, April 5, 2019, online: <https://www.whitecase.com/publications/article/chapter-7-legal-basis-processing-unlocking-eu-general-data-protection-regulation> (“Chapter 7: Legal Basis for Processing – Unlocking the EU General Data Protection Regulation”).
- “Chapter 8: Consent – Unlocking the EU General Data Protection Regulation”, White & Case, April 5, 2019, online: <https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation> (“Chapter 8: Consent – Unlocking the EU General Data Protection Regulation”).
- “Chapter 8: Trans-border Data Flows and Data Localization Requirements”, Smartblock Law, in *Big Data Law in Canada*, December 2019, online: <https://www.smartblocklaw.com/blog/big-data-law-in-canada-ch8> (“Chapter 8: Trans-border Data Flows and Data Localization Requirements in *Big Data Law in Canada*”).
- “Chapter 9: Rights of Data Subjects – Unlocking the EU General Data Protection Regulation”, White & Case, April 5, 2019, online: <https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation> (“Chapter 9: Rights of Data Subjects – Unlocking the EU General Data Protection Regulation”).
- “Children’s Privacy Threatened by Play Websites and Social Networking”, PIAC, November 4, 2008, online: <https://www.piac.ca/our-specialities/childrens-privacy-threatened-by-play-websites-and-social-networking/> (“Children’s Privacy Threatened by Play Websites and Social Networking”).
- “Commish ‘Frustrated for Canadian Citizens’ as Privacy Laws Lag”, October 8, 2020, The Wire Report (“Commish ‘Frustrated for Canadian Citizens’ as Privacy Laws Lag”).
- “Comparative Table of Personal Information Protection Laws”, Fasken, online: [https://iapp.org/media/pdf/resource-center/Comparative Table of Personal Information Protection Laws English.pdf](https://iapp.org/media/pdf/resource-center/Comparative%20Table%20of%20Personal%20Information%20Protection%20Laws%20English.pdf) (“Comparative Table of Personal Information Protection Laws”).
- “COVID-19 and Privacy: Artificial Intelligence and Contact Tracing in Combatting the Pandemic”, McCarthy Tetrault LLP (Barry Sookman), April 14, 2020, online: <https://www.mccarthy.ca/en/insights/blogs/techlex/covid-19-and-privacy-artificial-intelligence-and-contact-tracing-combatting-pandemic> (“COVID-19 and Privacy: Artificial Intelligence and Contact Tracing in Combatting the Pandemic”).
- “COVID-19 Pandemic Reveals Major Gaps in Privacy Law, Says Watchdog”, CBC news, October 8, 2020, online: <https://www.cbc.ca/news/politics/privacy-commissioner-annual-report-2020-1.5754930> (“COVID-19 Pandemic Reveals Major Gaps in Privacy Law, Says Watchdog”).
- “COVID-19 Realities Push Ontario Government to Launch Public Consultation to Improve the Province’s Privacy Laws”, McMillan LLP, August 19, 2020, online: https://mcmillan.ca/Files/224317_COVID-19_Realities_Push_Ontario_Government_to_Launch_Public_Consultation_to_Improve_the_Provinces_Privacy_Laws.pdf (“COVID-19 Realities Push Ontario Government to Launch Public Consultation to Improve the Province’s Privacy Laws”).
- “Current Landscape of Personal Information and Privacy Liability in Canada”, Wallace Folick LLP, February 2016, online: <https://www.dolden.com/wp-content/uploads/2016/06/166-Current-Landscape-of-Personal-Information-and-Privacy-in-Canada-February-2016.pdf> (“Current Landscape of Personal Information and Privacy Liability in Canada”).

- “Damages Under PIPEDA: A Purposive Approach and a New High Water Mark”, Canadian Privacy Law Review (Neil Wilson, Stevensons LLP), December 2013, online: <https://www.swlawyers.ca/wp-content/uploads/2019/08/Damages-under-PIPEDA-A-Purposive-Approach-and-a-New-High-Water-Mark-Canadian-Privacy-Law-Review-Neil-Wilson.pdf> (“Damages Under PIPEDA: A Purposive Approach and a New High Water Mark”).
- “Data Class Actions in Europe and Spotlights in Mexico, Russia and the US”, Hogan Lovells, December 12, 2019, online: https://www.hoganlovells.com/~media/hogan-lovells/pdf/2019/2019_12_12_data_class_actions_guide_15_low.pdf?la=en (“Data Class Actions in Europe”).
- “Data Commons & Data Trusts: What They Are and How They Relate”, Anouk Ruhaak, May 15, 2020, online: <https://medium.com/@anoukruhaak/data-commons-data-trust-63ac64c1c0c2> (“Data Commons & Data Trusts: What They Are and How They Relate”).
- “Data Trusts: Why, What and How”, Anouk Ruhaak, Medium, November 11, 2019, online: <https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34> (“Data Trusts: Why, What and How”).
- “De-identify, Anonymize and De-index: New Verbs and New Obligations!”, Fasken Martineau DuMoulin LLP, August 24, 2020, online: <https://www.fasken.com/en/knowledge/projet-de-loi-64/2020/08/24-depersonalisation-anonymisation-desindexation-nouvelles-obligations> (“De-identify, Anonymize and De-index: New Verbs and New Obligations!”).
- “Did the Supreme Court of Canada formally establish a new form of consent? Is ‘implied consent’ really ‘deemed irrevocable consent’?”, Canadian Privacy Law Blog (David T.S. Fraser), December 1, 2016, online: <https://blog.privacylawyer.ca/2016/12/did-supreme-court-of-canada-formally.html> (“Did the Supreme Court of Canada formally establish a new form of consent?”).
- “Digital Contact Tracing: The Trojan Horse in the Battle Over Data”, May 22, 2020, The Hill, online: <https://thehill.com/opinion/cybersecurity/499113-digital-contact-tracing-the-trojan-horse-in-the-battle-over-data> (“Digital Contact Tracing: The Trojan Horse in the Battle Over Data”).
- “Digital Finance Package: Commission Sets Out New, Ambitious Approach to Encourage Responsible Innovation to Benefit Consumers and Businesses”, European Commission, September 24, 2020, online: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684 (“EC: Digital Finance Package: Commission Sets Out New, Ambitious Approach to Encourage Responsible Innovation to Benefit Consumers and Businesses”).
- “Does Anonymization or De-identification Require Consent under the GDPR?”, IAPP (K. Elm Emam and M. Hinze), January 29, 2019, online: <https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/> (“Does Anonymization or De-identification Require Consent under the GDPR?”).
- “Emerging Models of Modern Data Governance”, Team BlockGeni, September 19, 2020, online: <https://blockgeni.com/emerging-models-of-modern-data-governance/> (“Emerging Models of Modern Data Governance”).
- “Essential Requirements for Establishing and Operating Data Trusts: Practical Guidance Based on A Working Meeting of Fifteen Canadian Organizations and Initiatives”, Vol. 5 No. 1 (2020): IJPDS Standard Issue, online: <https://ijpds.org/article/view/1353> (“Essential Requirements for Establishing and Operating Data Trusts”).
- “Facebook Fights Irish Privacy Watchdog’s Data-Transfer Curbs”, Bloomberg, September 11, 2020 (“Facebook Fights Irish Privacy Watchdog’s Data-Transfer Curbs”).
- “Factsheet: the European Data Strategy”, European Commission, February 2020, online: https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283 (“European Data Strategy FAQ”).
- “Finding our Way Through Privacy, Data Gaps and Pandemic Response”, Canadian Lawyer (Chantal Bernier), May 19, 2020, online: <https://www.canadianlawyermag.com/news/opinion/finding-our-way-through-privacy-data-gaps-and-pandemic-response/329733> (“Finding our Way Through Privacy, Data Gaps and Pandemic Response”).
- “GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act”, IAPP (Timothy Banks), May 2, 2017, online: <https://iapp.org/news/a/matchup-canadas-pipeda-and-the-gdpr/> (“GDPR matchup: Canada’s Personal Information Protection and Electronic Documents Act”).
- “GDPR Top Ten #1: Data Portability”, Deloitte, undated, online: <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-data-portability.html> (“GDPR Top Ten #1: Data Portability”).
- “GDPR vs CCPA”, Ropes & Gray LLP, undated, online: <https://www.ropesgray.com/~media/Files/PraxPages/CCPA/GDPR-vs-CCPA.pdf> (“GDPR vs CCPA”).
- “Guide to Doing Business in Canada: Privacy Law”, Gowling WLG, October 1, 2020, online: <https://gowlingwlg.com/en/insights-resources/guides/2020/doing-business-in-canada-privacy-law/> (“Gowling: Guide to Doing Business in Canada: Privacy Law”).
- “Implications of the ‘Data Fiduciary’ Provision in the Proposed New York Privacy Act”, New York Law Journal, February 28, 2020, online: <https://www.law.com/newyorklawjournal/2020/02/28/implications-of-the-data-fiduciary-provision-in-the->

- [proposed-new-york-privacy-act/?slreturn=20200911113837](#) (“Implications of the ‘Data Fiduciary’ Provision in the Proposed New York Privacy Act”).
- “Is Civic Data Governance the Key to Democratic Smart Cities? The Role of the Urban Data Trust in Sidewalk Toronto”, December 2020, *Telematics and Informatics*, Volume 55, online: <https://doi.org/10.1016/j.tele.2020.101456> (“Is Civic Data Governance the Key to Democratic Smart Cities?”).
- “Is the Clock ‘Tik Toking’ on Global Data Localisation? Could De Facto Localisation Become a Reality?”, Clifford Chance, August 20, 2020, online: <https://talkingtech.cliffordchance.com/en/data-cyber/data/is-the-clock--tik-toking--on-global-data-localisation-.html> (“Is the Clock ‘Tik Toking’ on Global Data Localisation?”).
- “Key Features of the GDPR”, Selvam & Selvam (IP law firm), June 24, 2019, online: <https://selvams.com/blog/key-features-of-the-gdpr/> (“Key Features of the GDPR”).
- Labor and Monopoly Capital*, H. Braverman, New York: Monthly Review Press, 1998 (“Labor and Monopoly Capital”).
- “Looking to Comply with GDPR? Here’s a Primer on Anonymization and Pseudonymization”, IAPP (Matt Wes), April 25, 2017, online: <https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/> (“Looking to Comply with GDPR? Here’s a Primer on Anonymization and Pseudonymization”).
- “Ontario Enters the Private Sector Privacy Realm: What the New Privacy Law Consultation Means for Business”, Torys LLP, August 24, 2020, online: <https://www.torys.com/insights/publications/2020/08/ontario-enters-the-private-sector-privacy-realm#:~:text=Unlike%20Qu%3%A9bec%2C%20British%20Columbia%2C%20and,the%20course%20of%20commercial%20activities> (“Torys: Ontario Enters the Private Sector Privacy Realm”).
- “Ontario Government Launches Consultation to Enhance Privacy Protections”, Blake, Cassels & Graydon LLP, August 17, 2020, online: <https://www.blakes.com/insights/bulletins/2020/ontario-government-launches-consultation-to-enhance> (“Ontario Government Launches Consultation to Enhance Privacy Protections”).
- “Ontario Launches Consultation for New Provincial Private Sector Privacy Legislation”, Osler, Hoskin & Harcourt LLP, August 13, 2020, online: <https://www.accessprivacy.com/e-news/2020/ontario-launches-consultation-for-new-provincial-p> (“Ontario Launches Consultation for New Provincial Private Sector Privacy Legislation”).
- “Ontario’s Privacy Consultation Could Lead to New Private Sector Data Protection Laws, But Not Everyone is Thrilled About it”, ItWorldCanada (Howard Solomon), August 17, 2020, online: <https://www.itworldcanada.com/article/will-ontarios-privacy-consultation-lead-to-a-private-sector-data-protection-law/434596> (“Ontario’s Privacy Consultation Could Lead to New Private Sector Data Protection Laws, But Not Everyone is Thrilled About It”).
- “OPC Happy With Tracing App, But Not With Privacy Law”, The Wire Report, August 28, 2020 (“OPC Happy With Tracing App, But Not With Privacy Law”).
- “Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy”, McCarthy Tétrault LLP, April 3, 2018, online: <https://www.mccarthy.ca/en/insights/blogs/snippets/parliamentary-committee-recommends-substantial-revisions-pipeda-part-5-adequacy> (“Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 5 – Adequacy”).
- “PIAC Final Written Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics: Review of PIPEDA”, PIAC, February 20, 2017 (“PIAC 2017 Final Submission to ETHI Review of PIPEDA”).
- “PIPEDA: A Constitutional Analysis”, Josh Nisker, Goodmans LLP, online: <http://goodmans.ca/docs/5CPIPEDA.pdf> (“PIPEDA: A Constitutional Analysis”).
- “PIPEDA v. GDPR: The Key Differences”, Endpoint Protector Blog (Andrada Coos), September 6, 2019, online: <https://www.endpointprotector.com/blog/pipeda-vs-gdpr-the-key-differences/#:~:text=Data%20breach%20notifications&text=The%20GDPR%20requires%20companies%20to,affected%20as%20soon%20as%20feasible> (“PIPEDA v. GDPR: The Key Differences”).
- “Preparing for the EU GDPR in Research Settings”, Johns Hopkins Medicine, May 22, 2018, online: https://homewoodirb.jhu.edu/files/2018/08/GDPR-Application-in-Research-Settings_JHU-Homewood.pdf (“Preparing for the EU GDPR in Research Settings”).
- “Privacy and Cybersecurity Bulletin”, Fasken, March 29, 2018, online: <https://www.fasken.com/en/knowledge/2018/03/bill-14-ontarios-new-privacy-law/> (“Fasken: Privacy and Cybersecurity Bulletin”).
- “Privacy Best Practices in a Pandemic Public Health Emergency”, Canadian Privacy Law Blog (David T.S. Fraser), April 10, 2020, online: <https://blog.privacylawyer.ca/2020/04/privacy-best-practices-in-pandemic.html> (“Privacy Best Practices in a Pandemic Public Health Emergency”).
- “Privacy Commissioner Again Upends the Consensus on Transfers for Processing In Aggregate IQ Investigation”, Canadian Privacy Law Blog (David T.S. Fraser), December 11, 2019, online: <https://blog.privacylawyer.ca/2019/12/privacy-commissioner-again-upends.html> (“Privacy Commissioner Again Upends the Consensus on Transfers for Processing In Aggregate IQ Investigation”).

- “Privacy Commissioner of Canada argues for rights-based privacy laws in Annual Report”, McCarthy Tetrault, January 23, 2020, online: https://www.mccarthy.ca/en/insights/blogs/techlex/privacy-commissioner-canada-argues-rights-based-privacy-laws-annual-report#_ftnref6 (“Privacy Commissioner of Canada Argues for Rights-based Privacy Laws in Annual Report”).
- “Privacy in Canada: A Public Interest Perspective – Address to the Rile Conference on Privacy and Bill C-54”, PIAC (Philippa Lawson), February 1999, online: <https://www.piac.ca/our-specialities/privacy-in-canada-a-public-interest-perspective/> (“Privacy in Canada: A Public Interest Perspective – Address to the Rile Conference on Privacy and Bill C-54”).
- “Privacy Update – Provincial Privacy Law Reform, Final CCPA Regulations and More”, Canadian Marketing Association (“CMA”), August 19, 2020, online: <https://www.the-cma.org/about/blog/privacy-update-provincial-privacy-law-reform-final-ccpa-regulations-and-more> (“Privacy Update – Provincial Privacy Law Reform, Final CCPA Regulations and More”).
- “Provincial Privacy Refreshers Underway in Ontario”, McCarthy Tetrault LLP, September 22, 2020, online: <https://www.mccarthy.ca/en/insights/blogs/canadian-employer-advisor/provincial-privacy-refresher-underway-ontario> (“Provincial Privacy Refreshers Underway in Ontario”).
- “Provincial Private Sector Privacy Law Being Considered in Provincial Consultation”, Law Times, August 26, 2020, online: <https://www.lawtimesnews.com/practice-areas/privacy-and-data/provincial-private-sector-privacy-law-being-considered-in-provincial-consultation/332722> (“Provincial Private Sector Privacy Law Being Considered in Provincial Consultation”).
- “Public Consultation on Ontario Privacy Law Reform for Private Sector”, Hicks Morely Hamilton Stewart Storie LLP, August 28, 2020, online: <https://hicksmorley.com/2020/08/28/public-consultation-on-ontario-privacy-law-reform-for-private-sector/> (“Public Consultation on Ontario Privacy Law Reform for Private Sector”).
- “Public Education Fact Sheet: De-identification and Anonymization of Personal Information”, PIAC, October 6, 2011, online: https://www.piac.ca/wp-content/uploads/2014/11/fact_sheet_faq_final_6oct2011_2.pdf (“Public Education Fact Sheet: De-identification and Anonymization of Personal Information”).
- “Quebec Plans Ambitious Overhaul of its Privacy Law”, Law in Quebec (Luis Millan), July 17, 2020, online: <https://lawinquebec.com/quebec-plans-ambitious-overhaul-of-its-privacy-law/> (“Quebec Plans Ambitious Overhaul of its Privacy Law”).
- “Quebec to Introduce the Most Punitive Privacy Laws in Canada – With Fines of Up to \$25 million”, Gowling LLG, June 9, 2020, online: <https://gowlingwlg.com/en/insights-resources/articles/2020/quebec-to-introduce-the-most-punitive-privacy-laws/> (“Quebec to Introduce the Most Punitive Privacy Laws in Canada”).
- “Québec’s Bill 64 proposes sweeping changes to its privacy regime”, Torys LLP (M. Reynolds, R. Shah, T.A. Reguly, G. Bertrand, and J. Stober), June 19, 2020, online: <https://www.torys.com/insights/publications/2020/06/quebecs-bill-64-proposes-sweeping-changes-to-its-privacy-regime> (“Québec’s Bill 64 Proposes Sweeping Changes to its Privacy Regime”).
- “Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR”, Dentons LLP, July 9, 2020, online: <http://www.dentonsdata.com/quebecs-new-privacy-bill-a-comparison-of-bill-64-pipeda-and-the-gdpr/> (“Quebec’s New Privacy Bill: A Comparison of Bill 64, PIPEDA, and the GDPR”).
- “Robots and Artificial Intelligence in Health Care,” I. Kerr, J. Millar, and N. Corriveau, in *Canadian Health Law and Policy*, 5th edition, 2017 (“Robots and Artificial Intelligence in Health Care”).
- “Schrems II’: Impact on Data Flows with Canada”, IAPP (Abigail Dubiniecki), August 14, 2020, online: <https://iapp.org/news/a/schrems-ii-impact-on-data-flows-with-canada/> (“Schrems II’: Impact on Data Flows with Canada”).
- “Schrems II: The Saga Continues”, McCarthy Tetrault, July 16, 2020, online: <https://www.mccarthy.ca/en/insights/blogs/techlex/schrems-ii-saga-continues> (“Schrems II: The Saga Continues”).
- “Strengthening Privacy for the Digital Age: Response to Proposals to Modernize PIPEDA”, Canadian Bar Association (“CBA”), December 2019, online: <https://www.cba.org/CMSPages/GetFile.aspx?guid=ef901bd8-d329-4d36-87e5-2298290a2b84> (“CBA’s Response to ISED’s Proposals to Modernize PIPEDA”).
- “Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’”, Canadian Anonymization Network (Canon), October 15, 2019, online: <https://deidentify.ca/wp-content/uploads/2019/10/CANON-Submission-ISED-Strengthening-Privacy-for-the-Digital-Age.pdf> (“Canadian Anonymization Network: Submission re: ISED’s ‘Strengthening Privacy for the Digital Age’”).
- “Supreme Court of Canada Decision Raises Interesting Issues About Jurisdiction Over Privacy-Impactful Technologies”, Teresa Scassa blog, July 15, 2020 (“Supreme Court of Canada Decision Raises Interesting Issues About Jurisdiction Over Privacy-Impactful Technologies”).
- “Switzerland – Data Protection Overview”, OneTrust DataGuidance, August 2020, online: <https://www.dataguidance.com/notes/switzerland-data-protection-overview> (“Switzerland – Data Protection Overview”).
- “Tech Companies Fail to Comply with New EU Regulations on Data Sharing, Survey Finds”, The Logic Briefing, September 28, 2020 (“Tech Companies Fail to Comply with New EU Regulations on Data Sharing, Survey Finds”).

“The Constitutionality of PIPEDA: A Re-Consideration in the Wake of the Supreme Court of Canada’s Reference re Securities Act”, former SCC Justice Michel Bastarache, June 2012, online: <http://accessprivacy.s3.amazonaws.com/M-Bastarache-June-2012-Constitutionality-PIPEDA-Paper-2.pdf> (“The Constitutionality of PIPEDA: A Re-Consideration in the Wake of the Supreme Court of Canada’s Reference re Securities Act”).

“The EU is Launching a Market for Personal Data. Here’s What That Means for Privacy.”, MIT Technology Review, August 11, 2020, online: <https://www.technologyreview.com/2020/08/11/1006555/eu-data-trust-trusts-project-privacy-policy-opinion/#:~:text=Its%20General%20Data%20Protection%20Regulation,new%20legislation%20around%20the%20world.&text=A%20data%20trust%20is%20a,a%20key%20asset%20for%20Europe> (“The EU is Launching a Market for Personal Data”).

“The GDPR and What it Means for Canada”, Privacy Canada (Ludovic Rembert), September 27, 2020, online: <https://privacycanada.net/gdpr-pipeda-guide/> (“The GDPR and What it Means for Canada”).

“The Governance of Data in a Digitally Transformed European Society”, M. Micheli et al, Joint Research Centre, European Commission, Italy, January 2019, online: https://www.researchgate.net/publication/330223608_The_Governance_of_Data_in_a_Digitally_Transformed_European_Society (“The Governance of Data in a Digitally Transformed European Society”).

“The New Ecosystem of Data Trusts”, Medium (Vince J. Straub), February 26, 2019, <https://medium.com/@vincejstraub/the-new-ecosystem-of-data-trusts-36901fc59010#:~:text=Examples%20include%20the%20Nesta%20Trust,arms%20length%20from%20political%20decisions> (“The New Ecosystem of Data Trusts”).

“The Privacy, Data Protection and Cybersecurity Law Review - Edition 6: Canada”, The Law Reviews (Shaun Brown, nNovation LLP), October 2019, online: <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210002/canada> (“The Privacy, Data Protection and Cybersecurity Law Review - Edition 6: Canada”).

“The Schrems II Decision: Implications and Challenges for Canada”, Colin J. Bennett, July 16, 2020, online: <https://www.colinbennett.ca/data-protection/the-schrems-ii-decision-implications-and-challenges-for-canada/> (“The Schrems II Decision: Implications and Challenges for Canada”).

“The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020”, ICLG (White & Case), May 7, 2020, online: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/1-the-rapid-evolution-of-data-protection-laws> (“The Rapid Evolution of Data Protection Laws: Data Protection Laws and Regulations 2020”).

“The Times They Are A Changin’: Canadian Privacy Law in the Private Sector”, Davies LLP, September 18, 2020, online: <https://www.dwpv.com/en/insights/Publications/2020/Canadian-Privacy-Law-in-Private-Sector> (“The Times They Are A Changin’: Canadian Privacy Law in the Private Sector”).

“Trust”, Investopedia (Julia Kagan), April 5, 2020, online: <https://www.investopedia.com/terms/t/trust.asp> (“Trust”).

“Trusted Secure Data Sharing Space”, Community Research and Development Information Services (“CORDIS”), European Commission, online: <https://cordis.europa.eu/project/id/871481> (“EC: Trusted Secure Data Sharing Space”).

“Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA”, Bennett Jones LLP, May 14, 2018, online: <https://www.bennettjones.com/en/Blogs-Section/Understanding-the-GDPR> (“Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA”).

“Voter Data and the Impact of Privacy Legislation Gaps on Cybersecurity of Elections”, Dr. Elizabeth F. Judge, Professor of Law and member of the Center for Law, Technology and Society at the Faculty of Law at the University of Ottawa, December 6, 2018, online: <https://konnect.serene-risc.ca/2018/12/06/voter-data-and-the-impact-of-privacy-legislation-gaps-on-cybersecurity-of-elections/> (“Voter Data and the Impact of Privacy Legislation Gaps on Cybersecurity of Elections”).

“Wealth and Private Client: Trust Basics”, Norton Rose Fulbright, June 2019, online: <https://nortonrosefulbright.com/media/files/nrf/nrfweb/knowledge-pdfs/trust-basics.pdf> (“Wealth and Private Client: Trust Basics”).

“What Exactly Is A Data Trust?”, Matthew Halliday, July 28, 2020, MaRS, online: <https://marsdd.com/news/what-exactly-is-a-data-trust/> (“What Exactly Is A Data Trust?”).

“What Is a Data Trust?”, McDonald, Sean, and Bianca Wylie, *Centre for International Governance Innovation* (“CIGI”), October 9, 2018, online: <https://www.cigionline.org/articles/what-data-trust> (“What Is a Data Trust?”).

“What is a Data Trust and Why are We Even Talking About It? Sidewalk Labs’ Magic Tricks”, Mariana Valverde, January 14, 2019, online: <https://cfe.ryerson.ca/blog/2019/01/what-data-trust-and-why-are-we-even-talking-about-it-sidewalk-labs%E2%80%99-magic-tricks> (“What is a Data Trust and Why are We Even Talking About It? Sidewalk Labs’ Magic Tricks”).

“Workplace Privacy, an Increasingly Important Issue in the Information Age”, Minken Employment Lawyers, online: <https://www.minkenemploymentlawyers.com/employment-law-issues/workplace-privacy-an-increasingly-important-issue-in-the-information-age/> (accessed September 21, 2020) (“Workplace Privacy, an Increasingly Important Issue in the Information Age”).

*** End of Document ***