

FINAL REPORT

**INSIGHTS INTO THE
PUBLIC'S ACCEPTANCE
OF GOVERNMENT USE
OF DATA**

NOVEMBER 17, 2021

DOCUMENT VERSION CONTROL

Version Number	Date of Issue	Author(s)	Brief Description
1.0	Aug. 31, 2021	Davis Pier Consulting	Initial draft
1.1	Sept. 2, 2021	Davis Pier Consulting	<ul style="list-style-type: none"> • Added Executive Summary and Recommendations • Added infographics to replace some text placeholders • Updated layout and formatting of document
1.2	Sept. 23, 2021	Davis Pier Consulting	<ul style="list-style-type: none"> • Updated layout and formatting of document • Further refinement of content • Incorporation of feedback from DDI WG members
1.3	October 21, 2021	Davis Pier Consulting	<ul style="list-style-type: none"> • Incorporated feedback from ISED and DDI WG co-chairs
1.4	November 17, 2021	Davis Pier Consulting	<ul style="list-style-type: none"> • Incorporated feedback from TBS, Chair of the Joint Councils Privacy Sub-Committee, CRA, and MSDO.

Table of Contents

- Executive Summary5**
- Project Background and Overview 10**
- Geographic Insights Scan..... 13**
 - Key Insights 13
 - Approach 14
 - Insights 15
 - Additional Desktop research 23
- Literature Review 32**
 - Key Insights 32
 - Approach 32
 - Acceptance of Data Use and Sharing across Geographic Regions 33
 - Acceptance of Data Sharing by Purpose 43
 - Trust among Vulnerable Populations 47
 - ‘Privacy Calculus’ a Contributing Factor to Public Acceptance of Data Sharing 48
 - Research Gaps 49
- Overview of Key Legislation 51**
 - Key Insights 51
 - Introduction 51
 - Approach 52
 - Overview of key legislation 54
 - Key similarities in legislation 56
 - Insights & Notable differences for sharing with other jurisdictions or governments within Canada 57
- Recommendations..... 65**
- Appendix A: Sources for Literature Review..... 72**
- Appendix B: Jurisdictions Contacted for the Geographic Insights Scan 75**
- Appendix C: Sources for Geographic Insights Scan..... 76**
- Appendix D: CSA Model Code..... 78**
- Appendix E: Sources for Overview of Key Legislation 80**
- Appendix F: Summary of Canadian Privacy Legislation 82**



01.

Executive Summary

Executive Summary

As governments seek to enhance service delivery, more focus is being placed on embracing the principles of Human-Centred design. To support this user-centric design approach, there is a need to collect and retain information (in many cases, personal information) from the citizens being served. By adopting initiatives such as *Tell Us Once*, information can be collected from a citizen and then shared with other areas or departments that are providing services to them. This information can also play a vital role in the planning and provisioning of services, thereby informing governments about what citizens want (and don't want) out of a service delivery experience.

The use of data to improve service delivery within and across levels of government in Canada raises issues such as responsible use of data and analytics, and the protection of the personal information of citizens. Privacy legislation requires notification of a party's authority to collect personal information, and the purpose for the collection. If that personal information is then used, disclosed, and/or retained for reasons not consistent with that purpose, then consent must be obtained. However, concepts such as implied consent and "consistent use" can create situations in which information is legally collected, used and shared without a citizen's direct knowledge.

One additional aspect to be considered is not so much whether citizen's personal information **can** be legally used and shared by government, but more so whether citizens think government **should** be using and sharing their information.

The Institute for Citizen-Centred Service's (ICCS) Data-Driven Intelligence (DDI) Working Group has undertaken an initiative to develop a comprehensive understanding of public acceptance for the use and sharing of data for the improvement of public services within and across levels of government. As a part of this initiative, Davis Pier was commissioned to undertake research into the public's level of acceptance of government data use and sharing, with a focus on the use of data to improve services. This project is intended to inform the future direction of intergovernmental use of data in Canada, as well as to guide future research on barriers to data sharing for public services across government.

It should be noted that, while the focus of this report may be on use of data for digital channels, it is vital that services are always designed to be made available to those with no online or digital access, such as vulnerable or marginalized populations.

Approach

To provide comprehensive insights into public levels of acceptance of data sharing from a range of sources and perspectives, the project team conducted research in three parts:

- **Geographic Insights Scan:** Desktop research and stakeholder consultation across Canadian and with international jurisdictions to identify approaches for addressing public acceptance

of the sharing and use of data and personal information to improve government service delivery.

- **Literature Review:** Summary and analysis of peer-reviewed and high-quality grey-literature sources with a focus on providing comparative levels of acceptance of data sharing across geographic regions and demographic groups.
- **Legislative Scan:** Analysis of the legislation governing the collection, use and disclosure of personal information across Canadian Provinces / Territories / Municipalities and the Government of Canada, noting key similarities and notable differences.

These separate approaches enabled the collection of a diverse range of perspectives which provide comprehensive insights into the public acceptance of data sharing for the improvement of public services in Canada.

Key Insights

The three methods of inquiry used provide a diverse range of insights into public levels of acceptance around government's use of data, both in a Canadian and international context. The key insights from each section include:

Geographic Insights Scan

- A majority of the jurisdictions consulted as part of this project do not formally monitor the public's perception of government use of data. Despite this, most jurisdictions still collect ad-hoc information about public perceptions from a range of different sources - for example, as part of consultations related to a policy initiative or legislative change.
- Stakeholders identified two issues of greatest public concern: a perception that government uses public information for undisclosed secondary purposes, and frustration over having to provide the same information to government multiple times. These public concerns represent two increasingly divergent population groups - one that is placing more trust in government, and one that has declining trust in government.
- In line with the findings above, the effects of the COVID-19 pandemic ranged significantly from increased acceptance of government use of public information to declining trust and confidence in government.

Literature Review

- Public levels of acceptance of data use and sharing can differ substantially across geographic regions. Canadians are found to have generally higher levels of trust in government sharing of health data than those in the UK, though lower than those in Australia and the US.

- Levels of acceptance in data collection, use and sharing differed substantially based on the intended use and recipient of data. For example, the use of data for the purpose of improving public safety or health is more acceptable than for general services and administration. Similarly, doctors and health researchers are generally more trusted for data collection and sharing than other parties, including governments and private companies.
- Though there is limited data available in a Canadian context, research suggests that trust in data use and sharing is generally lower among vulnerable populations, including members of the LGBTQ and BIPOC communities.

Legislative Scan

- There are 41 separate statutes, each with its own regulations, addressing privacy at the Federal, Provincial and Territorial (F/P/T) levels. Only three jurisdictions have distinct legislation for municipalities: Ontario, Saskatchewan, and Nova Scotia. All other municipalities fall under the respective provincial *freedom of information and protection of privacy* legislation.
- An extensive review of the public and private sector legislation in Canada has shown that to fully benefit from the digital economy and share data for administrative and non-administrative purposes, legislative reform is necessary. Political will, an embedded mandatory review of legislation and an active Information and Privacy Commissioner office helped some jurisdictions achieve substantial changes to their public sector legislation.

Recommendations

Leveraging these key insights, the following recommendations have been proposed for consideration by the ICCS, falling under three overarching themes:

Theme 1: Understanding levels of public trust

- A** Engage directly with the public across Canada to better understand their levels of acceptance of government data use.
- B** Encourage P/T/M governments to establish formal monitoring of Canadians' levels of public acceptance of data use and sharing (with a focus on identifying differences in levels of acceptance across different geographic regions, urban-rural/small centres, and demographic groups).

Theme 2: Strengthening the relationship between government and the public

- C** Support government to take specific actions to promote transparency to build or regain trust.

- D** Encourage governments to allow citizens to opt into a “Tell Us Once” approach, where data may be shared with other government departments for a set of agreed uses, in alignment with public sector legislative contexts within Canada.
- E** Advocate for the prioritization of Indigenous Data Sovereignty by government organizations.

Theme 3: Improving internal government operations

- F** Encourage governments to establish centralized Data Authorities, in alignment with public sector legislative contexts within Canada.
- G** Educate public servants on what information they can and cannot share (secondary usage) and the requirements for consent, according to privacy legislation in their jurisdiction.
- H** Encourage and support F/P/T/M legislative reform to enable the secondary uses of data not currently allowed.

All recommendations are outlined in detail in Section 6 of this report.



02.

Project Background and Overview

Project Background and Overview

The Data Driven Intelligence Working Group (DDIWG) works under the direction of the Joint Councils (the Public Sector Service Delivery Council (PSSDC) and the Public Sector Chief Information Officer Council (PSCIOC)) to explore the framework of issues impacting the ability of governments to improve the client experience, leveraging open data and advanced data analytics to improve service delivery.

While citizens may be used to providing information to public entities to receive goods and services, they are not necessarily comfortable with **not** knowing where their information is stored, with whom it is shared, and how it is (or will be) used. Many are providing information without even knowing the extent of the use of their information under the auspices of consistent use. This is especially true of marginalized and vulnerable populations, who may be more focused on receiving support for themselves and their families and less on understanding their rights under privacy legislation.

The topic of consent is complex, and further complicated by the coverage/use of concepts such as *express* and *implied* consent which differ in their application at the Federal and Provincial/Territorial/Municipal levels. For example, service delivery concepts such as *Tell Us Once* are dependent upon informed consent, and would need to be provisioned to be in compliance with both local and national governing laws. A deeper analysis of consent, while warranted, is not within the scope of this report. However, it would be instructive to explore it further in a future phase of this work.

Knowing a citizen's level of acceptance of how broadly a public body may use their information is vital to the design of an effective, user-centric service. This creates a need for governments that the ICCS is responding to through this project, to better understand just how the public feels about public sector organizations using their data.

In response to a request from the Joint Councils, the DDIWG has commissioned the development of this research to explore the current context of public acceptance for the use of data to improve services within and across levels of government. Insights gained from this research are expected to help inform the Canadian governments' use of citizen data in future programs and services. It will also provide a foundation for future projects that will identify and provide options for addressing legislative, policy and data sharing barriers to designing, implementing and delivering services across governments in Canada.

Much of the content in this report relates to attitudes, needed innovations and important trends in data sharing. It is important to note that the scope of this research is restricted to **citizens'** levels of acceptance of government's data sharing, specifically. Future phases of this work should explore uses of citizen data (and their level of acceptance) by industry, and what legislative oversight / constraints exist to provide control and transparency.

The project team has approached conducting this research project through the completion three distinct phases:

1. A **Geographic Insights Scan** of approaches to addressing public acceptance of the sharing and use of data and personal information to improve government service delivery. This includes consulting with Canadian Federal/Provincial/Territorial/Municipal committees that may be addressing similar questions, and international jurisdictions that may have or may also be dealing with these issues.
2. A **Literature Review** of existing academic and public opinion research on the public's acceptance and trust of the use of data and personal information for the provision of government services. This includes identifying significant variances across geographic locations or demographic groups, and also looks at attitudes within vulnerable and minority populations.
3. An **Overview of Key Legislation** governing the collection, use and disclosure of personal information across Provinces/Territories/Municipalities and the Government of Canada. Key similarities and notable differences in collection, use and disclosure within and to other jurisdictions are identified, along with changes being made to legislation to better facilitate data exchange. A look at best practices in select international jurisdictions is also included.

The information gathered by this project is needed to inform future direction around intergovernmental data use in Canada. It will also provide foundational material for a future project to investigate and outline options to address legislative, policy and data sharing barriers to integrated and seamless service delivery across levels of government.

By design, this project is driven by a need for better integration and information sharing within and between jurisdictions while considering citizens' attitudes toward and acceptance of that sharing of their personal information. **While the focus of this report may be on use of data for digital channels, it is vital that services are always designed to be made available to those with no online or digital access, such as vulnerable and marginalized populations.**



03.

Geographic Insights Scan

Geographic Insights Scan

Key Insights

- Information & Privacy Commissioners (IPC) and Government Information Access and Privacy (IAP) offices from all 13 Provinces and Territories, and eight Chief Digital Officers (CDO) were invited to provide input for this report.
 - Respondents included 5 IPC offices, 12 government IAP offices, and 5 CDO offices agreed to meet or provide written feedback.

- Of the stakeholders that responded:**

Over 50% were not aware of any provincial government departments or organizations that are formally monitoring public general acceptance of government's use of data.

Less than 50% are gauging public opinion on data use on a project-to-project basis.

Over 50% reported that public trust in government (in general) has increased since the start of the pandemic. However, **over 33%** reported that public mistrust of government's use of data during the pandemic has grown.

Approximately 25% reported a key concern for the public being a perception that government uses data for secondary uses without consent.

Approximately 20% reported that the public is growing tired of having to provide their information multiple times to government.

- Consultations and research conducted for this report have surfaced 11 insights, grouped according to five themes:

Theme 1: Government awareness of public acceptance

- 1.1** More than half of the stakeholders we interviewed were not aware of government organizations formally monitoring public acceptance of the use of their data
- 1.2** Despite a widespread lack of formal monitoring, most jurisdictions still collect information about public perception from a range of different sources
- 1.3** Some jurisdictions are looking to introduce monitoring of public acceptance

Theme 2: Issues of greatest public concern

- 2.1** There appear to be two issues of greatest public concern - a perception that government uses public information for undisclosed secondary purposes and frustration at having to provide the same information to government multiple times
- 2.2** Facial recognition technology is a public concern in some jurisdictions but not in others

Theme 3: Change in public level of acceptance

- 3.1** The effects of the COVID-19 pandemic ranged significantly from increased acceptance of government use of public information to declining trust and confidence in government

Theme 4: Geographic trends

- 4.1** Information and Privacy Commission (IPC) concerns vary across the country
- 4.2** The citizens who are most vocal about privacy concerns vary across and within jurisdictions
- 4.3** Public interest in privacy has increased across the country in recent years

Theme 5: Barriers

- 5.1** It can be difficult to establish data sharing initiatives in government
- 5.2** Political will is critical to the success of open data initiatives

These 11 insights are detailed below, along with supporting desktop research.

Approach

A scan of Canadian jurisdictions' approaches to, and projects addressing, public acceptance for the use of data and the sharing of personal information to improve service delivery was performed.

The initial group of stakeholders identified for direct consultation, based upon their expected exposure to the public, were Information & Privacy Commissioners (IPC), and Government Information Access and Privacy (IAP) offices from all 13 Provinces and Territories. Near the end of the research period, the offices of eight Chief Digital Officers (CDO) across Canada were sent a survey based upon the questions asked during direct consultations in order to help bolster the results of this scan.

Overall, five of the thirteen IPCs, all but one government IAP office, and five CDOs agreed to meet or provide written feedback. Of the five CDOs that replied, two were available for follow-up consultation. (A full list of jurisdictions involved in the consultations is included in Appendix B.)

To facilitate consistent and fulsome engagement, a standard set of questions was prepared and used for all interviews. This question set also formed the basis of the survey sent to CDOs. This question set was designed to inquire about public acceptance of government use of the following types of data or information:

- Sharing of personal information for administrative purposes such as for authentication or verification in support of service delivery to clients.
- Use of service-related data and information for non-administrative purposes, such as program evaluation or statistical analysis, including using new technologies and methods of artificial intelligence.

In addition to the Canadian jurisdictions that were consulted, further web-based research was conducted on initiatives being undertaken by Canadian and select international jurisdictions to improve public trust in data usage and facilitate better data sharing within, and by, government.

The criterion for selecting the international jurisdictions was opportunistic – it included those specifically identified by the ICCS in the early stages of the project, and also those jurisdictions that caught the attention of the project team during the course of their research for this report.

A full list of all sources used to complete the Geographic Scan is included in Appendix C.

Insights

Consultations and research conducted for this report have identified 11 key insights, organized into five themes:

Theme 1: Government awareness of public acceptance

1.1 More than half of the stakeholders we interviewed were not aware of government organizations formally monitoring public acceptance of the use of their data.

Insufficient resourcing was cited by one stakeholder as a driving factor in the decision not to monitor public perception within their organisation. Another stakeholder said that they were unsure about how they would survey citizens. Although some jurisdictions track the number of complaints made about government, this does not necessarily correlate directly with public acceptance.

While not an example of monitoring of acceptance of data use per se, one government that has been formally monitoring public trust is that of New Zealand.

Example: New Zealand

The New Zealand Government actively monitors levels of trust in government – both through ongoing, longitudinal data collection and specific point-in-time studies. The Kiwis Count public trust survey measures the trust and confidence of New Zealanders in government. The survey is conducted quarterly with 1,000 people, and helps government to improve the services it provides. Results are shared with the public and given to agencies to help identify areas where issues may be developing and remedial action might need to be taken. The survey gives the government a valuable insight into New Zealander’s views, trust and confidence in government and its role in society.

Headline measures as of April 2021 include:

- 79% of New Zealanders trust public services based on their personal service experience.
- Trust in the public sector brand is 63%, down from its latest high of 69%.
- Trust in the private sector brand is 50%, up from 48% and a new high.

(Source: <http://publicservice.govt.nz/our-work/kiwis-count-survey/> with historical reporting available at <https://www.publicservice.govt.nz/our-work/kiwis-count-survey/kiwis-count-archive-including-the-survey-methodology/>)

1.2 Despite a widespread lack of formal monitoring, most jurisdictions still collect information about public perception from a range of different sources

Almost half of the stakeholders we interviewed said that they gauge public opinion on a project-by-project basis - for example, during public consultation on a policy or legislative initiative. One stakeholder also told us that they formally monitor of the public's perception of private companies' use of their data and draw inferences about what that could mean for government.

Other common tactics included conducting secondary analysis of public correspondence and questions submitted to government and monitoring media releases and other publications. One publication cited as particularly useful was the annual Information and Privacy Commission report.

Example: British Columbia

British Columbia has conducted periodic public engagement in recent years regarding access to information and privacy. Examples of such public engagement include:

- Summer 2021 - Invited British Columbians to provide input on provincial public sector privacy laws around data residency, fees and other issues.
- Summer 2021 - Invited leaders of First Nations to participate in an online questionnaire to gain the unique perspectives of Indigenous people on access to information and privacy.
- Spring / Summer 2021 - Minister responsible for FOIPPA held a number of roundtables with stakeholder groups.
- Summer 2021 - Held targeted engagement of stakeholders and rightsholders regarding government collection of race-based data.
- Fall 2019 - Hosted citizen roundtable around government use of personal health information (facilitated by PopData BC).
- 2018 - Invited British Columbians to provide input to help shape government's next steps regarding the Freedom of Information and Protection of Privacy Act (FOIPPA) and asked people to discuss issues such as penalties for contravening FOIPPA, fees for access to information, and the kinds of information they would like to see government make available without the need for a formal Freedom of Information (FOI) request.
- Spring 2018 - Minister responsible for FOIPPA held a number of roundtables with stakeholder groups

1.3 Some jurisdictions are looking to introduce monitoring of public acceptance

Several jurisdictions are actively looking to introduce mechanisms to monitor public acceptance of government data use. Examples include a citizen's panel that can be used to conduct proactive research, a Smart City Board comprised of members of the public, and routine public opinion

polling. These mechanisms could also support the development of policy initiatives and help to gauge public trust and confidence in government more generally.

Theme 2: Issues of greatest public concern

2.1 There appear to be two issues of greatest public concern - a perception that government uses public information for undisclosed secondary purposes and frustration at having to provide the same information to government multiple times

Of all the public concerns stakeholders told us about, there were two that stood out as common across jurisdictions.

Approximately a quarter of stakeholders we interviewed said a key concern in their jurisdiction is the perception that government uses information for secondary purposes that the public did not consent to. This includes a perception that public information is freely shared between departments, or even with the private sector. Stakeholders told us that marginalized communities in some jurisdictions may be particularly concerned about this issue, and experience some of the lowest levels of trust in government. Overall, we heard that the public would like more government transparency - including an “open by default” approach regarding the authority public information is collected under and for what purposes.

One stakeholder also told us that the public appears more concerned about government use of their information than the private sector’s. Some citizens may not understand the benefits that data sharing can facilitate, including better service delivery.

Another key concern, expressed by approximately a fifth of stakeholders, is that the public does not want to provide government with the same information multiple times. Stakeholders told us that the public is calling for better data integration and a “tell us once” approach.

These two concerns may be seen as antagonistic - and addressing them both could prove challenging. On the one hand, the public is seeking assurance that their information is only being used by government for specific purposes, and on the other hand people want better data integration and are willing to consent to more information sharing across departments. Government transparency will be key to addressing and reconciling these two concerns.

Other public concerns we heard about, which had less cross-jurisdictional commonality, fell into three main categories - management of public information, trust and accountability, and the COVID-19 pandemic:

1. Management of public information

- How public information is kept safe
- How people can access their own information
- Late access to information requests

2. Trust and accountability

- Mistrust of law enforcement, particularly following specific violent incidents
- Indigenous data sovereignty
- Mistrust of government's use of facial recognition technology
- Concerns that individual citizens will be able to be identified from data that should be anonymized

3. The COVID-19 pandemic

- The government's response to the COVID-19 pandemic, which some people feel was rushed and failed to account for privacy considerations
- Vaccine passports, and whether they breach privacy considerations
- Poor treatment of citizens and employees in long-term care facilities
- Contact tracing applications that monitor the movement of individuals

Example: Ontario

Indigenous data sovereignty has been a consistently raised concern regarding use of public information - or even aggregated data - to support service delivery. Populations who have been historically excluded or negatively targeted had concerns about the effects of automated decision making. In Ontario, a Data Authority that follows the First Nations Information Governance Centre guidelines is being created to oversee data collection and use. It will also help to ensure that data-driven technologies benefit Indigenous populations.

Example: New Brunswick

As New Brunswick is a small Province, rural areas and postal codes have the potential to pinpoint participants. Citizens have raised concerns previously of having their views be associated with where they live - for example, by providing postal code with a survey response.

2.2 Facial recognition technology is a public concern in some jurisdictions but not in others

Stakeholders from two jurisdictions specifically mentioned that facial recognition technology is a key public concern - particularly regarding drivers' licensing and how facial recognition data is being stored and used. One stakeholder felt that the concern likely results from unfamiliarity with the technology, how it works, and what it can be used for.

Conversely, stakeholders from three jurisdictions told us that facial recognition is not an area of public concern, or is a peripheral issue only. These jurisdictions may be less advanced than others in their use of the technology, leading to lower public exposure and awareness. On the other hand, people in these jurisdictions may be more accustomed to facial recognition technology and therefore less concerned.

Theme 3: Change in public level of acceptance

The vast majority of stakeholders discussed the change in public acceptance in the context of the COVID-19 pandemic. This may be because most jurisdictions do not formally monitor levels of acceptance, in addition to the fact that the pandemic has had such a significant impact on government and the public in general.

3.1 The effects of the COVID-19 pandemic ranged significantly from increased acceptance of government use of public information to declining trust and confidence in government

More than half of the stakeholders we interviewed told us that public trust in government has increased in their jurisdiction since the start of the COVID-19 pandemic. We heard that citizens now want to interact with government online more, including for driver licensing requirements, accessing health services, registering for organ and tissue donation, and making administrative updates to their personal information.

Stakeholders also told us that the public is increasingly interested in more seamless data integration across government departments, for example through a single digital identity. Several stakeholders cited broad support for an electronic vaccine passport in their jurisdictions.

On the other hand, over a third of stakeholders told us that mistrust in government has increased since the pandemic. We heard that public concerns have elevated in general and trust has been eroded, due in part to increased government information gathering for vaccine registries and vaccine passports. One stakeholder told us that people in their jurisdiction feel

the government's approach to the pandemic was too rushed, and they are concerned that major policy changes were made in an emergency. Another stakeholder discussed perceived ethical issues around the use of COVID isolation hubs.

We also heard that, while the public wants to see government services match the way they live their lives, people are apprehensive about how easy it will be for their privacy to be breached. In response to these concerns, one jurisdiction is slowing its use of analytics to inform policy decisions and another has elevated privacy as a key government-wide priority item.

Even within single jurisdictions, stakeholders told us that the public exhibits highly divergent attitudes toward government. Vaccine passports were cited as an example of a particularly polarizing topic.

Example: New Brunswick

There was very little pushback from the New Brunswick public regarding additional collection of information during the pandemic. While mandatory travel registrations at the border initially garnered public attention, the key concern was inconvenience rather than a lack of trust. This may be attributable to an older, more compliant population that is more trusting of government.

Example: Saskatchewan

A recent survey showed that a minority of Saskatchewan residents are willing to share their personal information online to streamline their service experience. Respondents were also highly concerned about their personal information being compromised online.

Additionally, two groups of respondents are extremely concerned about information being compromised: those who are very willing to share information, and those who are very against sharing of information. This suggests that residents who freely share their information for convenience recognize the risks of doing so but are willing to accept them to avoid hassles.



Approximately seven in 10 (69%) Canadians said their views of privacy and the protection of their personal information have not changed in any way since the start of the COVID-19 pandemic in March 2020. In contrast, one in three (29%) said their views have changed since March 2020.



Canadians in Atlantic Canada (59%) and Ontario (55%) were more likely to report being more concerned about the protection of personal information now than they were prior to the COVID-19 pandemic. In contrast, those in Quebec (49%) and the Prairies (50%) were, instead, more likely to report being more aware when providing personal information.

Figure 1:

Canadian citizens' concerns over the privacy of personal information during COVID.¹

Theme 4: Geographic trends

4.1 Information and Privacy Commission (IPC) concerns vary across the country

We heard about a range of different IPC concerns, which vary across the country. There were no concerns held by a majority or significant proportion of interviewees. Concerns we heard about included the following:

- Biases in artificial intelligence and predictive analytics / algorithms - particularly where they disadvantage minority groups;

¹ Source: 2020-21 Survey of Canadians on Privacy-Related Issues - Office of the Privacy Commissioner of Canada https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/

- Mistrust in private companies and their use of public information;
- Use of immunization records in vaccine passports;
- The mosaic effect, where disparate data sources are aggregated, largely from outside of the public sector, and to reidentify otherwise anonymized individuals;
- State surveillance tactics - including video, body camera use, exposure notification, facial recognition technology and biometrics; and
- Lack of government clarity and transparency - including plain language notices and consent forms.

Despite the fact that governments may over-collect public information, we observed a general recognition that this is unlikely to be for nefarious purposes.

4.2 The citizens who are most vocal about privacy concerns vary across and within jurisdictions

In one jurisdiction, we heard that privacy-savvy groups are more likely to correspond with government than individual citizens, who rarely get in touch. In another jurisdiction, middle-aged individuals are responsible for most correspondence with government. A third stakeholder told us that in their jurisdiction, rural populations are more likely to express concerns about privacy issues than city-dwellers.

Example: Ontario

The IPC has called for 26 privacy, security, access, and accountability measures to be built into a robust governance framework for body worn cameras (BWC). The board and the service fully or substantially addressed most of these recommendations and agreed to follow up on the remaining items. The framework that has emerged will help ensure that the public's needs for transparency and accountability are met while also respecting their reasonable expectation of privacy. Building on this experience and the input of other key stakeholders, the IPC is developing comprehensive BWC governance framework, which could serve as a model for all other police services that are using or considering using BWC programs in Ontario, helping ensure consistency across the province.

4.3 Public interest in privacy has increased across the country in recent years

Stakeholders across jurisdictions have observed an increase in public interest in privacy, including exponentially more requests for information in recent years. This may be attributable to the development of new technologies with privacy implications and a surge in media coverage of privacy issues. Despite the increase in public interest, we also heard that most citizens appear confused about the complexities of privacy legislation - including what government can and cannot do with public information.

Supplementing this insight, DIACC's Canadian Digital Identity Research 2020 report found that the familiarity with a digital identity is higher in Ontario, Manitoba and Saskatchewan. Albertans were

the most supportive of the digital identity concept. Compared to other regions Quebec continues to be the least concerned when it comes to their personal information being compromised online, and they were more likely to consider it very important that their provincial government move quickly on digital identity.²

Nationally, the Canadian Institute for Advanced Research (CIFAR) is leading the Government of Canada’s \$125 million Pan-Canadian AI Strategy, working in partnership with three provincial AI institutes, the Alberta Machine Intelligence Institute, Mila in Montreal, and the Vector Institute in Toronto. Announced in the 2017 federal budget, the strategy has four major goals: (1) increase the number of outstanding AI researchers and skilled graduates in Canada, (2) establish interconnected nodes of scientific excellence in Canada’s three major centers for AI, (3) develop global thought leadership on the economic, ethical, policy and legal implications of advances in AI, and (4) support a national research community on AI. The implications of this initiative for government’s use of personal information are important. As thought leadership and capacity for working in AI increases, the applications of AI to the programs and services offered by government will evolve. This will lead to increased need for data / information for developing and tuning algorithms and other tenets of AI. Commensurate with this innovation will come the need for legislative evolution to provide regulation over the development and uses of AI on personal information.

Theme 5: Barriers to Data Sharing

5.1 It can be difficult to establish data sharing initiatives in government

Stakeholders from four jurisdictions told us that data sharing initiatives are typically difficult to establish in government, despite widespread acceptance that they are critical to delivering seamless public services. Ambiguity around defining authorities, as well as overcoming legislative restrictions and structural government silos, were identified as contributing challenges. We also heard that jurisdictions without centralized privacy oversight or leadership find data sharing across departments particularly difficult.

Stakeholders from four jurisdictions also told us that it can be difficult to know how long consent

Example: Nunavut

Data collection and meaningful engagement with the population can be difficult in Nunavut, where communities are geographically dispersed across a large area. Poor internet connectivity in some areas is an exacerbating constraint. This can lead to a lack of data, or an inaccurate representation of key issues, which can influence the quality of data available.

² Source: DIACC Canadian Digital Identity Research 2020

to public information lasts, or when global consent has been provided. This impacts how it can be shared within and between government departments, particularly if new initiatives are introduced after the data was collected.

5.2 Political will is critical to the success of open data initiatives

We heard that open data and data sharing initiatives require ongoing political appetite in order to succeed. One stakeholder specified that political change during electoral cycles has disrupted progress around an open data initiative.

Additional Desktop research

The following section provides a summary of desktop research that highlights actions being taken by government, private sector, and not-for-profit organizations to improve public trust in data usage. It focuses primarily on Canadian jurisdictions, but also includes several international leading practices from Australia, Estonia, the United Kingdom and New Zealand.

Enhancing digital government upskilling opportunities

Upskilling in digital government is increasing across Canada, as demonstrated by the three examples identified below. This is key to supporting increased public trust in government.

1. Canadian School of Public Service

The Canada School of Public Service is developing a blueprint for a Digital Academy that can be recreated in regions across Canada with strong emphasis on partnering with provincial and municipal governments, learning institutes (universities and colleges) and the private sector. It is also collaborating with the Policy Community Partnership Office to identify competencies related to digital/data literacy among the IT and policy communities.

2. Global Affairs Canada

Global Affairs Canada has developed a Data Analytics Training pilot program as part of its overall data strategy to increase data capacity among employees to make greater use of data in evidence-informed policymaking.

3. Statistics Canada

Statistics Canada is working closely with 12 educational institutions with data scientist/specialist programs to seek out data scientists as part of their departmental HR strategy. The agency also offers Research Data Centres as a place to engage and collaborate with the data science community for experimentation and innovation. (Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service).³

³ Source: <https://www.canada.ca/en/privy-council/corporate/clerk/publications/data-strategy.html>

Introducing a pan-Canadian approach to safe, secure digital identity

The Treasury Board of Canada Secretariat (TBS) is working with Innovation, Science and Economic Development Canada (ISED) and other departments and jurisdictions to develop a pan-Canadian approach to digital identity and the acceptance of trusted digital identities across jurisdictions and government. The goal is to allow Canadians and Canadian businesses to log in with their provincial trusted digital identity to access federal government services in a timely and secure way. They also developed an Algorithmic Impact Assessment to help assess and mitigate the risks associated with deploying an automated decision system.⁴

The *Treasury Board Directive on Automated Decision Making* is a mandatory policy instrument which applies to most federal institutions. It sets out the requirements that must be met by federal institutions to ensure responsible and ethical use of automated decision systems including those using AI.⁵ Standards to enable interoperability and recognition between federal government departments, provinces, territories, municipalities, and industry partners will make this possible.

Interoperability and Standards

The Pan-Canadian Trust Framework (PCTF) is a set of criteria and guidelines to ensure that public and private sectors abide by a common, agreed-upon set of rules to trust and accept each other's digital identities.⁶ Federal, Provincial and Territorial governments continue to work together to evolve the Public Sector Profile of the PCTF to assess digital identity programs and to accept trusted digital identities as issued by these digital identity programs to improve service delivery to Canadians. The Digital Identity and Authentication Council of Canada (DIACC), furthermore, continues to roll out PCTF tools and processes to support more broadly across the economy. Additionally, trust frameworks in other jurisdictional contexts, such as the European Union, United Kingdom, and elsewhere, continue to emerge.

The establishment of Digital Identity standards has progressed in Canada. In July 2020, the First Edition of CAN/CIOSC 103-1: Digital Trust and Identity was approved by the Standards Council of Canada (SCC) as a national voluntary standard for Canada. In February 2021, the SCC launched a request for proposal (RFP) to develop a national technical specification for digital credentials and digital wallets.

⁴ Source: Trusted Digital Transformation Considerations for Canadian Public Policy January 2019

⁵ Source: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>

⁶ Source: 2020-08-08 Digital-ID-General-with-CIOSC-Standard-Draft (EN)

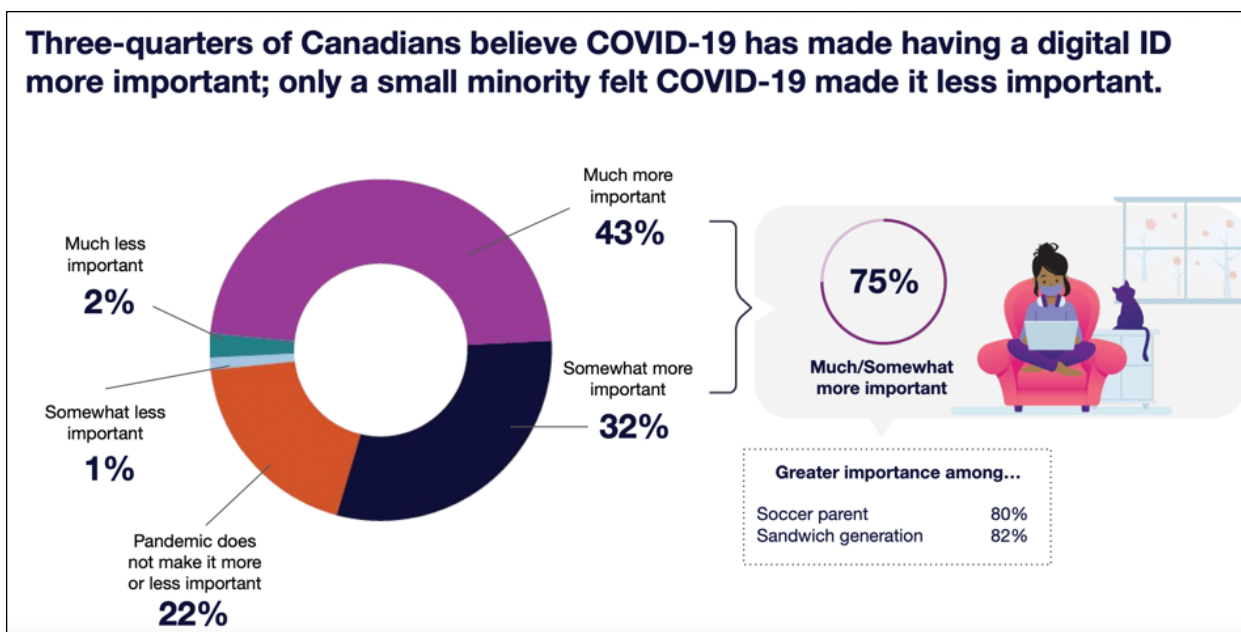


Figure 2: Canadian citizens' interest in having a digital ID.⁷

Australia

Three million Australians and half of all Australian businesses are now using digital identity. This is integrated across jurisdictions with New Zealand's digital identity system, with other countries like Singapore to follow. To build public trust, Australia has focussed on digital identity being voluntary, requiring informed and knowledgeable consent, and data minimization considered throughout.

The Digital Transformation Office (DTO) has also applied a user-centred service design approach to this work. This has involved taking an outside-in view to recast the project as a human experience. By observing, gleaning, experiencing, understanding, and empathizing with what people really do, think and use as they carry out their lives, the DTO is building services that citizens will use and establishing a more trusting relationship with the public.

Estonia

In Estonia, every citizen owns a digital identity and electronic signature. Estonia has legislated internet access as a human right and over 90 per cent of its population is online. The Estonian example suggests that e-governance is most accepted in small countries, overcoming

⁷ Source: DIACC Canadian Digital Identity Research 2020

dysfunctional or challenging past communication infrastructure, with a young population that shares high trust in institutions.

United Kingdom

The United Kingdom's Data Advisory Board, led by the Chief Executive of the Civil Service and Cabinet Office Permanent Secretary, aligns efforts to make the best use of data across government, such as initiatives to keep sensitive data secure, ensure common security standards, and make it easier for citizens to view and correct data about themselves, and refines ethical principles for data science techniques.

The UK is also committed to realising the benefits of digital identity, without creating identity cards. Earlier this year they published a draft of the UK Digital Identity and Attributes Trust Framework, like Canada's Pan-Canadian Trust Framework.

The framework shows how organisations can be certified to provide secure digital identity services; they will have to go through an assessment process with an independent certification body. It also states how data can be shared between organisations and announces the government will start testing the framework in partnership with service providers.⁸

They are also developing and piloting a new 'One Login for Government' system that will make it easier for everyone to access government services, with users only having to provide data to prove their identity once and protecting privacy throughout.⁹

Improving seamless service delivery

Improving service delivery is one of the most important ways to enhance public trust in government – simply by demonstrating high performance.

Direct Deposit and Address Information Sharing Initiative

A joint Government of Canada project, the Direct Deposit and Address Information Sharing Initiative (DAISI), is geared to enabling a "Tell Us Once" experience by sharing basic client information across organizations to streamline the process for Canadians to update their information—reducing time and confusion and providing consistency. With consent, Canadians' banking information will be updated for all CRA benefits and credit programs, such as the GST/HST credit, the Canada Child Benefit, the working income tax benefit, and their income tax refund. This information is shared with ESDC to update Canada Pension Plan information.¹⁰

⁸ Source: <https://www.gov.uk/government/news/next-step-in-plans-to-govern-use-of-digital-identities-revealed--2>

⁹ Source: <https://www.gov.uk/government/groups/data-advisory-board-and-data-leaders-network>

¹⁰ Source: Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service 2019

Calgary

The City of Calgary has integrated data from novel sources, including the Closed-Circuit Television system for Calgary Transit, into their overall data on opioid-related incidents. According to the City, "Overdose reporting correlates with high social disorder locations, primarily along the C-Train lines."

When incidents occur on Calgary Transit property, approximately one third of cases are reported using the HELP phone system and approximately 50 per cent are reported by Transit operators or through CCTV monitoring at the Transit Operations Center. In response to this escalating issue, Transit and Alpha House are piloting an approach that pairs a Downtown Outreach Addictions Partnership (DOAP) team outreach worker with a Transit peace officer. This team will operate on the C-Train system and proactively monitor locations with high social disorder and reported overdoses.¹¹

Bloomberg Philanthropies

Bloomberg Philanthropies works to ensure better, longer lives for the greatest number of people by focusing on five key areas: the arts, education, the environment, government innovation, and public health. Bloomberg launched *What Works Cities (WWC)* in 2015 under its government innovation key area. Prior to 2015, there were only a few US cities that had adopted a data driven approach to improve decision-making; many believed data-driven government was only for largely populated cities.¹²

WWC provides a growing national network of cities with a standard of excellence for data-driven local government (the WWC Standard), technical assistance from each of its expert partner organizations, peer learning opportunities to support and scale the adoption of data-driven approaches to pressing problems and government operations, and a suite of online trainings and webinars design to build city staff capacity. Any city with a population of at least 30,000 is eligible to access WWC resources.

Cities enrolled in the program and certified by BT have achieved the following:

- Performance management: The percentage of cities monitoring and analyzing their progress toward key goals has more than doubled (from 30% to 75%)
- Public engagement: The percentage of cities engaging with residents on a goal and communicating progress has more than tripled (from 19% to 70%)

¹¹ Source: The Opioid Crisis and Response: Update to Council and Senior Administration, City of Calgary, June 21, 2018

¹² Source: <https://www.bloomberg.org/>

- Releasing data: The percentage of cities with a platform and process to release data to residents has more than tripled (from 18% to 67%)
- Taking action: The percentage of cities modifying existing programs based on data analytics has more than doubled (from 28% to 61%)

Approximately 70% have reported that their cities are systematically using data-informed decision-making to respond to the COVID-19 crisis. Nearly 90% of cities report better using data to engage residents and/or community stakeholders.

When the WWC network was first developed, there were one or two people in each city government designated to support data-driven projects through the technical assistance that WWC provided. In the past six years there has been a sea change in the breadth and depth of data skills across cities. Today, WWC works with more than 11 city leaders in each city on average on projects. Cities have also moved from limited centers of data expertise, located in a specific role or department, to widespread use. In the city officials' survey, more than half of participating cities reported having spread data practices to eight or more departments or agencies.¹³

Digital Nations Initiative

The Digital Nations is a collaborative forum of the world's leading digital governments that aims to use technology to improve citizens services in Canada and globally. Canada is currently one of ten member countries. The other members are Estonia, Israel, Korea, New Zealand, United Kingdom, Uruguay, Mexico, Portugal, and Denmark. They lead digital government transformation for the benefit of citizens by:

- Developing digital policies and practices;
- Sharing these approaches and best practices with other member nations;
- Advancing all member nations' international influence; and,
- Strengthening relationships, building expertise, and connecting digital leaders globally.

Each year, Digital Nations member countries meet to share knowledge and expertise at working-level, Chief Information Officer-level and Ministerial-level meetings. Canada currently participates in the Digital Nations' thematic groups on artificial intelligence, digital identity, and data. Canada chairs the thematic group on greening government IT.

¹³ Source: Closing the Data Gap: How Cities Are Delivering Better Results for Residents A Monitor Institute by Deloitte report, in collaboration with What Works Cities June 2021

Estonia

Estonia operates the Citizen's Virtual Assistant, which is a voice based interactive tool that can link an individual to services. This has streamlined its operations as the government receives over 30,000 requests a year regarding police and border controls alone.¹⁴

As a result of all these initiatives and innovations Estonians' trust in their Parliament and government is much higher than the EU average. The Eurobarometer shows that more than half of the Estonian people, 51 percent, trust the government, which is 1 percent lower than last year. In the European Union on average, the state government is trusted by just 29 percent of the population.

The level of trust in national government among EU member states is higher only in the Netherlands (52 percent), Sweden (54 percent) and Malta (56 percent).¹⁵

Enhancing indigenous data sovereignty

The British Columbia provincial government passed the Declaration on the Rights of Indigenous Peoples Act (Declaration Act) into law in November 2019. The Declaration Act establishes the UN Declaration as the Province's framework for reconciliation, as called for by the Truth Reconciliation Commission's *Calls to Action*. This historic legislation was developed in collaboration and consultation with Indigenous partners, and aims to create a path forward that respects the human rights of Indigenous peoples while introducing better transparency and predictability in the work government shares with them. It requires development of an action plan to achieve this alignment over time and requires regular annual reporting on progress to the Legislature, providing transparency and accountability to monitor progress. In addition, the legislation allows for flexibility for the Province to enter into agreements with a broader range of Indigenous governments, and it provides a framework for decision-making between Indigenous governments and the Province on matters that impact their citizens.

Engaging citizens in decision-making

Service Alberta has launched an online consultation seeking stakeholder input on a number of privacy-related issues, including:

- Access to and control of one's personal information when interacting with government and private sector organizations
- The importance of clear and informed consent, data portability, and the right to be forgotten
- The need for greater transparency, such as plain language privacy statements

¹⁴ Source: <https://www.ria.ee/en.html>

¹⁵ Source: Eurobarometer Public Opinion in the European Union 2014
<https://europa.eu/eurobarometer/screen/home>

- The desire for legal requirements for collecting, using, and disclosing de-identified data
- Enhancing government oversight to ensure public and private sector organizations protect personal information as new technologies emerge.¹⁶

The province of Saskatchewan has done a lot of work with public engagement and proactively seeking input from citizens. This is intended to increase trust in government, as consultations have indicated that nearly three in four citizens somewhat or very concerned about their information being compromised online.¹⁷

Monitoring social license

A 2018 study by Statistics New Zealand, the primary department responsible for data collection led by the Chief Data Steward, looked at government's social license to make decisions about the management and use of the public's data. It was aimed at ensuring New Zealanders have trust and confidence in the way their data is managed.

The study found that:

- Most people who are familiar with Statistics New Zealand have some level of trust in what it does, as 85.5 percent of people who knew about its work have at least some trust in the organization.
- The less people knew about Statistics New Zealand, the less trust they had in the organization. Only 16.3 percent of those who had 'little knowledge' about Statistics New Zealand also had high trust in the organization.
- 39.9 percent of people don't know enough about Statistics New Zealand to give their informed trust to the organization.¹⁸

A 2016 study by the New Zealand Government on public attitudes to data integration found that:

- Participants generally expected information provided to government departments to be shared with other government departments.
- People appeared to gauge acceptability primarily on the need for the information. That is, how the data would be used and by whom.
- People were interested in the value of data integration, whether the benefits would outweigh the costs and risks, and how privacy and other risks might be mitigated.
- People felt that integrated data systems could be more reliable, current, and accurate than those currently used, and could result in more informed, fair, efficient, and effective decision-making and service provision.¹⁹

¹⁶ Source: <https://www.jdsupra.com/legalnews/everybody-is-jumping-on-the-privacy-1873356/>

¹⁷ Source: DIACC Canadian Digital Identity Research 2020

¹⁸ Source: <https://www.stats.govt.nz/corporate/a-social-licence-approach-to-trust>

¹⁹ Source: <https://www.stats.govt.nz/corporate/public-attitudes-to-data-integration>



04.

Literature Review

Literature Review

The following summarizes the key findings of a review of academic and grey literature exploring public acceptance and trust regarding use of data and related topics, with a focus on use of data in a public sector context.

Key Insights

- There is currently limited academic and grey literature exploring the levels of support for government use of data. The available literature suggests that levels of support and trust in Canada varies quite substantially according to the purpose or benefit of data sharing, with significantly higher levels of acceptance for the purpose of identifying fraud and making policy decisions, relative to comfort with using data for intelligence gathering.
- In qualitative studies conducted in Ontario and British Columbia, there was general concern around the potential for detrimental outcomes or misuse of data, and particularly for vulnerable members of the community, including members of the LGBTQ community and indigenous populations.
- Research across international geographies highlights that Canadians are less inclined to support sharing of data by government and healthcare professionals than those in the UK. Other research suggests that Canadians have lower trust in government use and sharing of data than those in Australia and the United States.
- In general, support for data sharing is higher for the purposes of improved personal safety, healthcare, medical research, and public health. Support is generally slightly lower for the purpose of government policymaking and decision making, and substantially lower for for-profit purposes, such as marketing.
- Evidence supports the 'Privacy Calculus Theory', which suggests that individuals approve of the sharing of personal information where they perceive that the positive benefits outweigh the negative outcomes of doing so. This has been demonstrated in the context of support for the use and sharing of personal data for the purpose of contact tracing to slow the spread of the COVID-19 virus.
- Although there is a strong body of international literature exploring the influences on trust and support for data sharing, there are significant research gaps which would need to be explored to build a comprehensive understanding of public acceptance of data sharing in a Canadian context. Particularly, there are gaps in data on the levels of trust across different geographic regions, and demographic groups.

Approach

This literature review focused on identifying academic and grey literature which explores public acceptance and trust regarding use of data and related topics, with a focus on data use in a public

sector context. To collect the largest spectrum of relevant publications from a range of sources and publications, a literature search was conducted using a range of electronic libraries, including, Science Direct, Springer Link, SAGE Journals, ScienceOpen, SSRN: Social Science Research Network, JSTOR: Journal Storage as well as Google Scholar (to ensure the identification of both peer-reviewed and other sources). Search strategies used subject heading terms appropriate for each database and key words relevant to public acceptance and trust in government use and sharing of personal data. Sources were selected for inclusion in this review based on their ability to provide valuable and unique insights for the topic of interest, as well as the robustness of the research methods applied. These resources were reviewed and analysed to provide a concise review of the literature which currently exists on public acceptance of government data sharing. The insights from these resources have been arranged into themes in the following review. These include public acceptance by geographic region, intended data sharing purpose and demographic factors (such as acceptance among vulnerable populations). While these themes are intersecting, this thematic grouping provides a structure for some of the key insights from the identified literature. In addition, we also identify some current research gaps which have been identified through the course of this literature review.

Acceptance of Data Use and Sharing across Geographic Regions

Although no sources were identified which provide a comprehensive comparison of public acceptance of data sharing across geographic regions, several studies were identified which compared attitudes across a small number of countries, or across a single country. The following section seeks to summarise the most relevant of these studies to provide an opportunity to contrast relative levels of trust and acceptance of government collection, use and sharing of data.

Public Acceptance of Data Sharing by Purpose in Canada

The *2020-2021 Survey of Canadians on Privacy-Related Issues* commissioned for the Office of the Privacy Commissioner of Canada provides recent and valuable insights into public opinion of government collection of data in Canada (Office of the Privacy Commissioner of Canada, 2021). The study looked at Canadians' level of acceptance with data collection and use by method and purpose, as well as by demographic factors such as age. This found that Canadians are most comfortable with personal information being collected from online sources such as social media posts, for the purpose of investigating potential fraud, with 57% stating they would be 'comfortable' or 'very comfortable' with this. This dropped to only 45% if the data were collected for the purpose of making decisions about government programs and services. Yet this differed quite significantly by age, with 62% of 16- to 24-year-old respondents stating that they supported this, compared to 38% of those aged over 55 years.

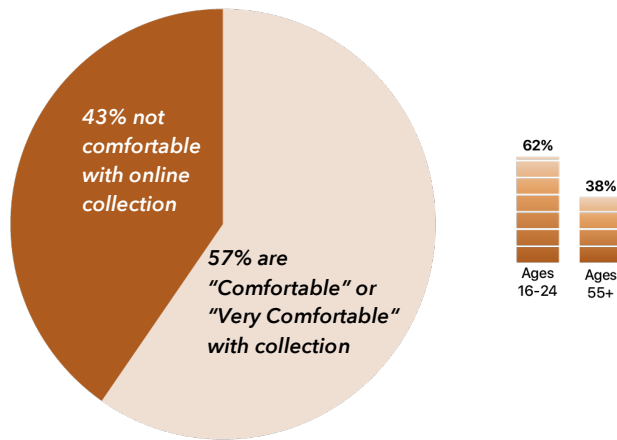


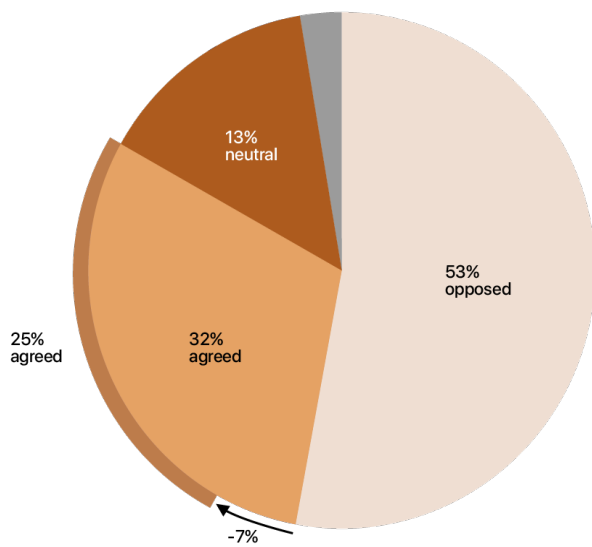
Figure 3: Canadians' comfort level with the online collection of information

Canadians are most comfortable with personal information being collected from online sources such as social media posts, for the purpose of investigating potential fraud.

This drops from 57% to only 45% if the data were collected for the purpose of making decisions about government programs and services.

Comfort levels differed quite significantly by age, with 62% of 16- to 24-year-old respondents stating that they supported this, compared to 38% of those aged over 55 years.

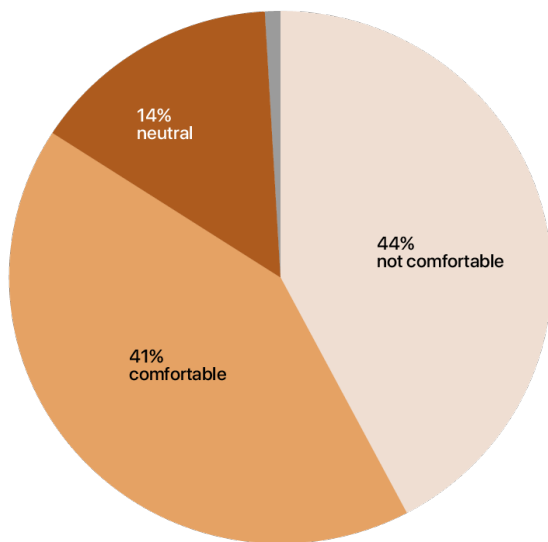
The study also identified that there is limited support for the collection of personal data for intelligence-gathering purposes. When asked whether “the government of Canada should have powers to collect and use citizens’ personal information as part of intelligence-gathering activities”, most respondents (53%) were opposed to the statement, while 32% agreed and 13% were neutral. The percentage of those who agreed with the statement declined to only 25% when it was stipulated that these activities would mean that “Canadians have to give up some personal privacy.” There was also a lack of consensus on acceptance of the government collecting personal information from financial institutions for the purpose of making economic decisions, such as for taxation and spending. Overall, 44% of Canadians were not comfortable with this use, 41% stated that they were comfortable, and 14% were neutral. Significantly, 63% of Canadians stated that they feel confident that the federal government respects their privacy; an increase from 55% in 2018. This was higher than trust in businesses, which sat at 45%. Interestingly, a majority (69%) of respondents stated that their views on privacy and the protection of personal information have not changed since the start of the pandemic. Of the 29% who stated that their views *had* changed, 48% stated that they were more concerned about protection of personal information.



When asked whether “the government of Canada should have powers to collect and use citizens’ personal information as part of intelligence-gathering activities”, most respondents (53%) were opposed to the statement, while 32% agreed and 13% were neutral.

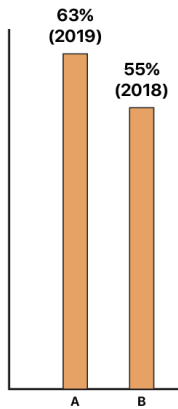
The percentage of those who agreed with the statement declined to only 25% when it was stipulated that these activities would mean that “Canadians have to give up some personal privacy.”

Figure 4: “Should the government of Canada collect and use citizens’ personal information for intelligence-gathering purposes?”



There was also a lack of consensus on acceptance of government collecting personal information from financial institutions for the purpose of making economic decisions, such as for taxation and spending. Overall, 44% of Canadians were not comfortable with this use, 41% stated that they were comfortable, and 14% were neutral.

Figure 5: “How comfortable are you with government collecting personal information from financial institutions for making economic decisions?”

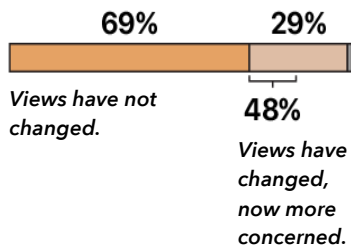


63% of Canadians stated that they feel confident that the federal government respects their privacy; an increase from 55% in 2018. This was higher than trust in businesses, which sat at 45%.

Figure 6: Canadians' Confidence that the Canadian Government respects privacy.



A majority (69%) of respondents stated that their views on privacy and the protection of personal information have not changed since the start of the pandemic.



Of the 29% who stated that their views had changed, 48% stated that they were more concerned about protection of personal information.

Figure 7: Canadians' views on privacy and the protection of their information.

British Columbia

In 2018, qualitative research was undertaken in Vancouver, British Columbia to seek public advice and insights regarding the use and sharing of linked data for research, focusing on the processes and regulations required to release data (Teng, Bentley, Burgess, O'Doherty, & McGrail, 2019). In this research context, they defined data as linked datasets from sources including patient-reported information, genomic information, data from wearable devices and social media. The research was conducted by Population Data BC, in collaboration with researchers at the University of Guelph and the University of Edinburgh. The research sought to provide a broad representation of the British Columbian community and held in-person consultation across a multiple-day event with 28 participants. This research found that in general, British Columbians were supportive of research using linked data due to its potential value to society. This was particularly strongly supported in

the context of research for public health emergencies. One of the primary areas of concern around data linkage for research was the potential for harmful impacts on populations studied, particularly in the case of vulnerable and marginalized populations (e.g., children, Indigenous communities). In management of such risks, respondents viewed that there needed to be proportionate governance which balanced risks with the need for efficient decision-making. Participants proposed that increasing transparency of data access would increase trustworthiness in data access processes. There was also concern around private corporations' involvement in research, and the motivating factors for research being out of alignment with the public good. Overall, participants specified a desire for improved efficiency of data request information to support more research, on the stipulation that sufficient protections are in place to protect security and privacy.

Ontario

In 2015 and 2017, eight focus groups were held with 65 members of the public in Ontario to learn more about the general public's attitudes toward users and uses of linked administrative health data held by ICES (Parica, Nunes du Melo, & Schull, 2019). The ICES is a non-profit corporation that conducts health outcomes research using data collected through Ontario's system of publicly funded healthcare. Specifically, they *"work with data sets that are created by linking person-level data from different data sets (e.g., prescription drugs, hospital admissions, mortality) then removing or coding identifying information so that research and analyses can be performed while protecting privacy"*. Reflecting the findings of the research conducted in British Columbia, this study found general support for the use of linked administrative health data for the purpose of conducting health research, though this general acceptance was conditional on context. The authors identified that one of the major conditions of acceptance of use of linked data was the need for assurance around privacy and security. Specifically, while de-identification of data was appreciated and a valuable step to privacy and security, that increasing the number of parties able to access data was still considered to increase the risk of privacy and security breaches. Additionally, support for use of the data was strongest when respondents agreed that there was a tangible public benefit associated. Conversely, support was weakest when it was seen that the outcomes could be misused or could disadvantage vulnerable populations. Similarly, there was substantially less support for the inclusion of the private sector in research studies using linked personal data, with some participants only approving of this where there would be reciprocal benefits to the public from their involvement (e.g. lower drug prices). Notably, there was not a consensus on the need to obtain consent when health data was de-identified, with mixed views on whether consent is necessary in this context. Through this research, the authors conclude that if researchers focus on conducting studies which *"have a clear public benefit and respect and address public concerns about privacy and private sector involvement, public support is likely to increase, enhancing the impact and the sustainability of research based on linked administrative health data."*

Canada and the United Kingdom (UK)

A recent study explored the perceived trustworthiness of specific social actors in Canada and the UK, and the impact of these on public willingness to consent to donating data to be used and shared for health research (Savic-Kallescoe, Middleton, & Milne, 2021). This research found that in general, Canadians had lower levels of public trust in data use and sharing than the UK. Indeed, 54% of UK citizens specified that they are generally trusting of at least two of the following potential data users: their doctor, any domestic doctor, their country's government, domestic for-profit researchers or domestic non-profit researchers. Comparatively, only 48% of Canadians specified that they were trustworthy of at least two of these potential data users. Interestingly, despite lower public trust levels, Canadians were *more* willing to donate their health data with these potential users. In Canada, 46% of Canadians were willing to donate their genomic data, compared to 40% of UK respondents. The authors suggest that these findings indicate that *“high levels of public trust do not guarantee high levels of willingness to donate; people are willing to donate even when they do not trust, and it cannot be guaranteed that those who do trust will also be willing to donate. Public trust is not sufficient for willingness to donate”*. They propose that factors such as trust in individual social actors, such as doctors and researchers, involved in the collection, management, storage and application of an individual's data may be more significant than overall public trust.

Canada, the UK, the US (United States) and Australia

In recognition of the potential for trust to play a role in shaping public attitudes towards genomic data sharing and big data initiatives, an online study was undertaken with 8,967 members of the general public in Canada, the UK, the US and Australia (Milne, et al., 2019). This research found that across all countries, participants were most likely to trust their doctor with their anonymized medical data, with 75% of respondents stating they would trust their doctor. People were less likely to trust any medical doctor (40%), or any researcher at a university in their country (34%), and much less likely to trust the government of their country (19%). Using these results, the researchers classified respondents into three categories: low overall trust (41%), variable trust (43%) and high trust (16%). Low trust is made up of those with moderate trust in one's own doctor and no trust in other organisations. Variable trust suggests high levels of trust in medical professionals, with moderate trust in university researchers and low trust in company researchers and one's own government. High overall trust is made up of those with high trust in all individuals/ organisations. Using these classifications, the researchers identified that participants in the Low Trust category were most likely to be from the UK, followed by Canada and the USA. Australians were least likely to fall in this category. People who fell into the high trust group were most likely to be from the US, followed by the UK and Canada. The research also identified that those who identified as male were more likely to fall into the high trust category, as well as those who were more highly educated. Persons under the age of 50 were more likely to fall into the high trust category, while those over 50 years were more likely to fall into the low or variable trust categories. Due to a low response rate from non-

white respondents, no conclusions were able to be drawn around the levels of trust. The authors conclude that across all countries, the extent to which the general public accept the sharing of health data varies by trust in the recipient, with the highest levels of trust in one's own doctor and the lowest levels of trust in companies and one's government.

The UK and the US

Another study looked at the comparative public attitudes towards data sharing and data access in healthcare across the UK and the US (Ghafur, Van Dael, Leis, Darzi, & Aziz, 2020). The two were selected for comparison on the basis that they are both high-income countries which have made substantial investments on health information sharing and data use but have markedly different health care delivery models. As such, the study sought to understand how these differences affect public attitudes towards data use and sharing. Notably, this research found that in general, willingness to share data was higher in the UK than the US. As displayed in *Figure 2*, willingness to share anonymized health information differed substantially dependant on which entity received the data. In both countries, willingness to share anonymized health data was highest when it would be shared with an individuals' doctor (UK: 75.4%, US: 60.6%), an academic or medical institution (UK: 50.3%, US: 25.5%), or a pharmacist (UK: 40.4, US: 41.2%). Willingness to share health data with one's government was relatively low in both countries, though substantially lower in the US (6.6%) than the UK (21.8%). The authors posit that *"the fact that distrust in the USA, which has a largely privatised system, was higher than in the UK, which has a socialised single-payer system, might indicate that patients are concerned that data might not be protected from commercial end-use."* In line with previous literature, this study suggests that people are least comfortable with sharing data for commercial purposes (Gostin, Halabi, & Wilson, 2018). In both the US and UK, less than 20% of respondents were willing to share anonymized personal health information with pharmaceutical companies, insurance companies and technology companies, even where those companies would use that data for health care improvement.

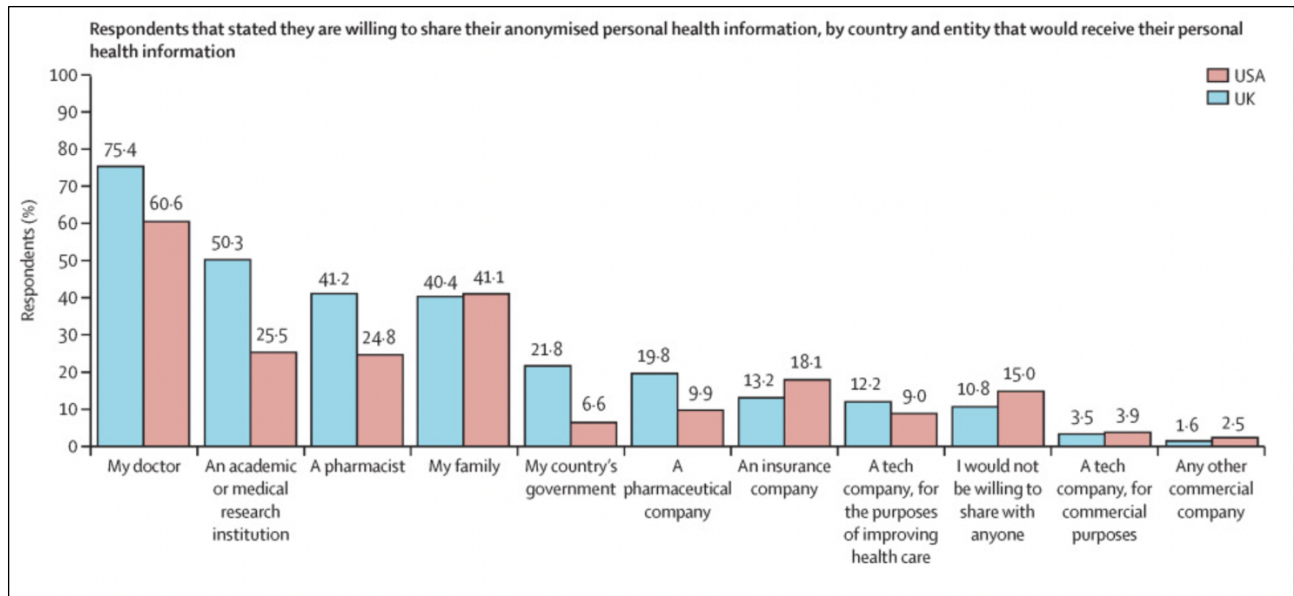


Figure 8: Willingness to Share Health Data by Entity in the UK and US²⁰

Europe

A comparative survey of attitudes to personal data sharing across a number of European countries was conducted in 2018 (Open Data Institute, 2018). The online study surveyed persons across Belgium, France, Germany, the Netherlands and the UK. The study found that across all countries, the vast majority of respondents stated that it was important that they trust an organisation or institution in order to be willing to share their personal data. The lowest proportion of respondents stating this view were in France, with 87% of respondents stating trust was important for data sharing, and the highest proportion were in the UK at 94%. This research also highlighted large differences in willingness to share data with different entities, as displayed in *Table 1*. Across the countries surveyed, people were most likely to trust healthcare providers and services with their information, followed by banks and financial institutions, and local and central governments. Reflecting the findings from the US and UK study, people were least willing to trust commercial entities, including marketing and advertising companies, insurance companies and retailers. Notably, there was a significant difference for levels of trust for the same entities between different countries. For example, the levels of trust in sharing data with central governments were relatively higher in the Netherlands (48%), the UK (37%) and Belgium (36%) than in France (17%) and Germany (16%).

²⁰ Source: Ghafur, S., Van Dael, J., Leis, M., Darzi, A., & Aziz, S. (2020). Public perceptions on data sharing: key insights from the UK and the USA. *The Lancet: Digital Health*.

Institution/Organization	Belgium	France	Germany	Netherlands	UK	Average
Central government	36%	17%	16%	48%	37%	31%
Local government (e.g. local council departments)	36%	19%	26%	53%	41%	35%
NHS & healthcare providers	60%	35%	37%	71%	64%	53%
Offline retailers (i.e. physical shops)	12%	8%	8%	11%	10%	10%
Online retailers (e.g. amazon)	12%	11%	15%	21%	22%	16%
Banks, building societies and credit card companies (e.g. Halifax, Barclays etc.)	48%	31%	34%	50%	57%	44%
Medical research charities (e.g. Cancer Research UK, MS Society etc.)	39%	15%	20%	43%	24%	28%
Marketing and advertising companies (e.g. saatchi & saatchi etc.)	5%	2%	2%	4%	2%	3%
Insurance Companies (e.g. Aviva, Direct Line etc.)	41%	27%	22%	40%	32%	32%
Social media organizations (e.g. LinkedIn, Facebook, Instagram etc.)	8%	5%	3%	8%	10%	7%
Universities	28%	14%	15%	21%	25%	21%
Family and friends	62%	55%	60%	61%	57%	59%
None of these	8%	16%	14%	8%	13%	12%
Don't know	8%	10%	7%	6%	7%	8%

Table 1. Willingness to Trust Organisations / Institutions with Personal Data by Country²¹

In addition, this study also asked respondents to identify which purposes for which they considered data to be useful. As highlighted by *Table 1*, the top response across all countries was that 'data is most useful when it helps keep me safe'. This was closely followed by support for the statement that 'data is useful when governments use it to understand and better serve society with improved public services'. Interestingly, attitudes towards this statement varied substantially by country, with respondents in the UK, Belgium and the Netherlands agreeing with statement at a rate of 51%, 41% and 37% respectively, while support in France and Germany was lower, at 29% and 24%. These differences reflect that public attitudes toward government data sharing for the improvement of public services can vary substantially according the specific geographic, political and social context.

Public Acceptance of Data Sharing between the Public, Private and Third Sectors in Scotland

In 2012, the Scottish Government commissioned research to explore the public acceptability of cross-sectoral data linkage for research and statistical purposes to understand levels of acceptance of data sharing between the public, private and not-for-profit sectors (Pagliari, et al., 2013). Using

²¹ Source: Open Data Institute. (2018). *Attitudes towards data sharing - Europe*. Open Data Institute.

qualitative methods, the research found that the public was, in principle, broadly supportive of data linkage, though this support was conditional on the purpose for which data would be used, and with whom it would be shared. First, the research identified significant concerns around privacy and security of data, and particularly the prevention of personal data being shared with commercial actors, such as private businesses. Concerns persisted even where data shared between stakeholders would be anonymized. Further, there was a strong view that research using shared data should only be conducted where some public benefit exists. As such, data sharing with private sector organisations was opposed on the basis that private companies would not act in the public interest. Similarly, sharing with the not-for-profit sector was viewed with skepticism due to the potential for sectional interests (i.e., interests of a particular group or organisation). One of the primary concerns highlighted by public consultation was the potential for data sharing to create negative outcomes for already marginalised members of the Scottish community. For example, LGBT participants were highly concerned that sexual orientation data could be misused, particularly in the event of a data breach. In drawing conclusions from the research, the authors highlighted the importance of *“approaching consultation as an on-going process rather than considering it as a one-off strategy to ascertain public attitudes and acceptability.”*

Singapore

A study in 2019 investigated Singaporean residents' level of trust and willingness to allow government collection of data, relative to their comparative levels trust in businesses (Ong & Ling Loo, 2021). Noting high levels of trust in their government, the study found that Singapore residents were still 'moderately concerned' with both government and business data collection. Notably however, they were less concerned with sharing data with government than businesses. Indeed, they were much more comfortable with their governments rather than businesses receiving personal contact information, work contact information, credit card information, demographic information, government identification, health history, location, social network friends' information and communication history. Of these data categories, residents were least comfortable with government access to their credit card information, personal contact information and communication history. When exploring levels of acceptance by demographic factors, the study found that increased income and education was associated with increased concern around government data collection. It also found that increased age was associated with lower concern with government access to location data, but unrelated with concern around health and social network data. The authors posit that this pre-existing level of concern for government data collection may have contributed to public concern and relatively low uptake of the Singaporean government's contact tracing technology, TraceTogether, during the COVID-19 pandemic response.

Acceptance of Data Sharing by Purpose

In addition to geographic differences in data sharing, research on public acceptance of data sharing has also focussed on the differences in public acceptance of data sharing for a range of different purposes. The contexts which are most relevant to the objectives of this literature, as well as those which have been most comprehensively studied are summarised below.

Data Sharing for Public Health

Prior to the emergence of the COVID-19 health crisis, public health was already one of the primary areas of research for public acceptance of data sharing. In particular, factors which influence public willingness to share genomic data with biobanks and other research bodies was well studied. This refers to the sharing of personal health data (such as DNA) to establish a 'bank' of genomic data to be used to build the scientific understanding of human health and diseases (Saskia C. Sanderson, 2017). The success and value of biobanks relies on access to large datasets, and therefore the consent of participants to provide 'broad consent'. This refers to the permission for researchers and institutions to utilise participants' data not only for a one-time, specified research objectives (narrow consent), but also for future, open-ended health research opportunities (Richter, et al., 2017). As such, a breadth of research has been conducted on the factors which affect public willingness to provide broad consent for the use and sharing of genomic data across institutions, including government organisations.

A significant study on public willingness to donate genomic data to a bio-bank conducted a survey across 36,262 individuals across 22 countries in 15 languages, with the intention of building an *"understanding of how members of the public, as donors of data, see and support the process of data sharing"* (Middleton, et al., 2020). The research found that across the full sample, the majority of participants were unwilling, or unsure, about donating their anonymous DNA and medical information for use by researchers. Further, they were most willing to provide information to a medical doctor, and least willing to donate to a for-profit researcher, particularly in Poland, Portugal and Germany (though with a much smaller difference in Egypt, India and Pakistan). Across all samples except India, trust in donating medical information to more than one user (i.e., doctor, researcher, government, company) and the willingness to donate data was closely correlated. In Canada, this association between trust across multiple actors and willingness to donate was one of the strongest associations, as displayed in *Figure 2*. The authors concluded that the variation between trust and willingness to donate genomic data suggests that trust in data users may not mean the same thing everywhere due to cultural and/ or circumstantial differences. They also found a strong association between a familiarity with genomic research, as well as awareness of benefits associated with biobank research (due to the presence of an inherited health condition, for example).

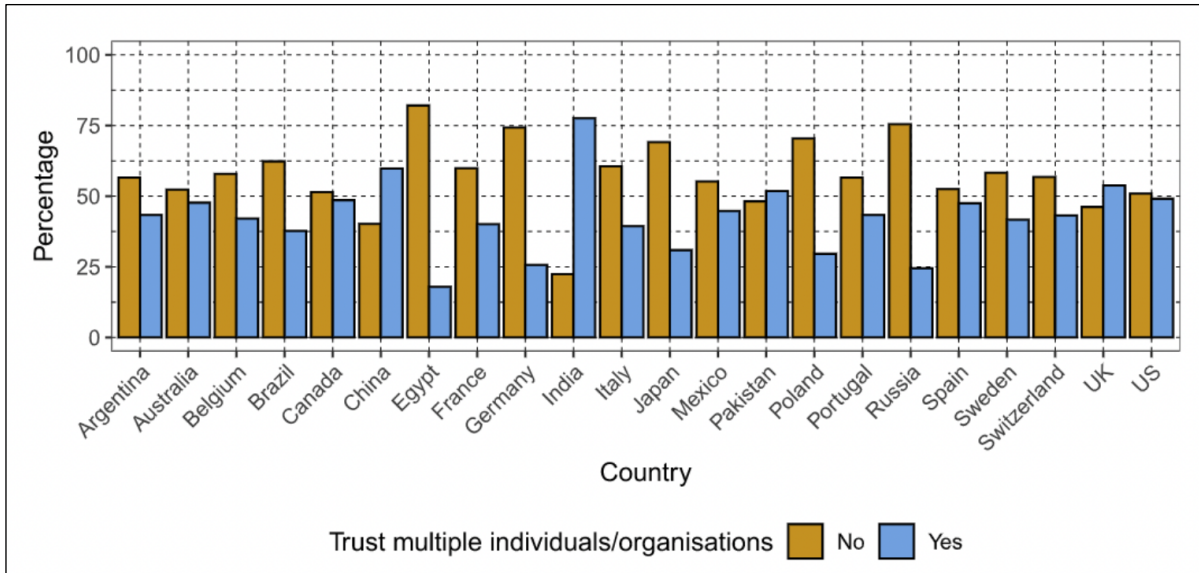


Figure 9: Trust in Donating DNA and Medical Information to More than One User, Stratified by Country²²

A range of other studies examined the factors affecting willingness to provide ‘broad’ consent across a range of geographies and contexts. For example, a systematic literature review of individuals’ perspectives on broad consent and data in the United States found that a minority of respondents supported a broad consent option where there was an option to grant narrow consent (e.g. study-by-study consent) (Garrison, et al., 2016). Willingness to grant broad consent increased if data were deidentified, as well as when the data were only to be shared between academic researchers. There was a lower willingness to provide broad consent where the data would potentially be shared across federal databases. The research also highlighted that racial and ethnic minorities often had more concerns about providing broad consent, though this information was incomplete. Similarly, the study highlighted that there is a dearth of information as to the influence of sociodemographic factors such as socioeconomic status and education on attitudes towards broad consent and data sharing. Another study looked at perspectives on broad consent in genomic research and biobanking in low- and middle-income countries (Tindana & de Vries, 2016). From this research, the authors recommended that the development of a robust governance framework for genomics and biobanking would require five key elements: respect, authentic community engagement and trust building, the preservation of privacy and confidentiality, feedback of results, and capacity strengthening.

²² Source: Middleton, A., Milne, R., Almarri, A., Anwer, Atutornu, J., Baranova, E. E., . . . Critchley, C. (2020). Global Public Perception of Genomic Data Sharing: What Shapes the Willingness to Donate DNA and Health Data? *The American Journal of Human Genetics*, 107, 723-752.

Data Sharing in the Pursuit of Contact Tracing for the COVID-19 Crisis

Over the past year, the COVID-19 crisis has stimulated research interest in the need to balance public health benefits with privacy concerns. This interest has been particularly driven by the potential for smartphone technologies to be used to collect data to assist public health efforts to track, trace and minimise the spread of the COVID-19 virus (Yasaka, Lhrich, & Sahyouni, 2020). Indeed, governments in several countries, including Singapore, Germany, the United Kingdom and Australia, have introduced smartphone 'tracking' applications over the past year (Lewandowsky, Dennis, Kashima, White, & Garrett, 2021). These 'apps' collect data on an individual's contacts in order to trace and notify people who may have come into contact with the virus. Although these initiatives have presented extensive opportunities to assist governments in tracing and minimising disease transition, they have sparked wide conversations around privacy and citizen acceptance of data sharing (French & Monahan, 2020). As such, several recent studies have focused on understanding citizens' perception and acceptance of data collection and sharing for the purpose of COVID-19 contact tracing.

In line with this focus, a study in Ireland sought to explore how citizens' perception of privacy and social benefit perceptions influence people's acceptance of data sharing for the purpose of contact tracing (Fox, Clohessy, van der Werff, Rosati, & Lynn, 2021). The study collected data both before and after the introduction of a nation-wide government contact tracing application, looking at factors including social influence, perceived benefits and privacy concerns. The study finds that social influence, social reciprocity and an individual's perception of the health benefits influenced their intention to use the application prior to its launch, and reciprocal benefits influenced usage over time. Interestingly, privacy concerns did not appear to influence usage intentions before or after the launch. This is not to suggest that privacy considerations were not a concern to citizens. Instead, the study's authors suggest that this indicates that the reciprocal and personal health benefits of the application, coupled with social influence, *outweighed* citizens' concern for privacy in the context of Ireland's national contact tracing application. Accordingly, they argue that when introducing policies, programs and technologies which rely on data sharing, policymakers should clearly communicate the benefits (both personal and reciprocal), as well as stress privacy protection measures and the need for information disclosure to achieve the stated objectives. As such, citizens can weigh the perceived costs and benefits of consenting to the use of their data, considering both the weight they place on social benefits and their privacy considerations.

Similar studies were also conducted in other regions. A study from Germany found that contact tracing application use rates were significantly higher among those who trusted the national government, the healthcare system and science in general, as compared with those who had low trust in those institutions (Munzert, Selb, Gohdes, Stoetzer, & Lowe, 2021). These findings align with research conducted in France which found that willingness to use a contact tracing application is strongly correlated with levels of trust in government (Guillon & Kergall, 2020). In the UK, a similar study found that public acceptance of contact tracking data collection and tracking technologies

sat between 60% and 70% in April of 2020 (Lewandowsky, Dennis, Kashima, White, & Garrett, 2021). The difference between these two reported levels was based on the extent to which privacy preserving measures were included in the proposed policy, such as the option to opt-out of data collection for contact tracing. This research found that the most significant association with acceptance for contact tracing technologies is an individual's trust in government, and specifically their trust in government's ability to safeguard privacy.

Data Sharing in the Context of a 'Vaccine Passport'

Vaccine passports refer to a digital or physical document which would enable the holder to demonstrate having received a COVID-19 vaccination, and thus be able to partake in activities such as international travel (Dye & Mills, 2021). Already, the European Union, Denmark, Israel and New York have introduced vaccine passports which enable access to a range of activities, and within Canada, the federal government has committed to the development of a vaccine passport for international travel. Even prior to the availability of a COVID-19 vaccine, researchers have been exploring the ethical, practical, legal and privacy considerations of vaccine passports, as well as public opinion on their use (Schlagenhauf, Patel, Rodriguez-Morales, Gautret, & Grobusch, 2021). In Canada, an Ipsos poll conducted in early May 2021 found that the public held strong support for the use of vaccine passports to enable access to a range of activities (Simpson, 2021). For example, 74% of Canadian supported the use of vaccine passports to visit a senior's facility. This remained at 72% for flying on an airplane, and 71% for flying internationally. Even for activities like attending outdoor concerts and stadiums, more than 66% of those surveyed either somewhat or strongly supported the requirement for vaccine passports.



74% of Canadian supported the use of vaccine passports to visit a senior's facility. This remained at 72% for flying on an airplane, and 71% for flying internationally. Even for activities like attending outdoor concerts and stadiums, more than 66% of those surveyed either somewhat or strongly supported the requirement for vaccine passports.

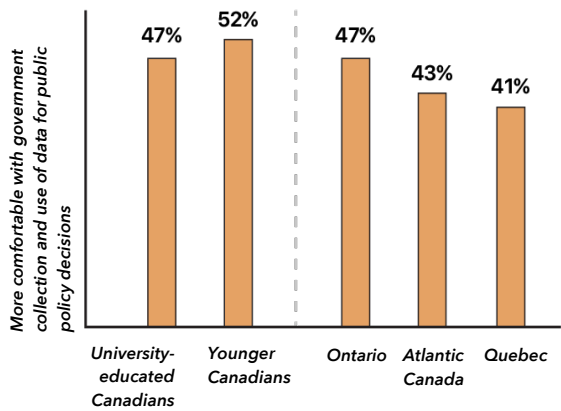
(Source: Simpson, S. (2021). Majority of Canadians Support Vaccine Passports for Variety of Indoor and Outdoor Activities. Toronto: Ipsos Public Affairs)

Another study conducted a rapid literature review of public acceptability of vaccine passports using 33 literature reviews from a breadth of countries, including Germany, the UK, US, Australia, Canada, Nigeria, Poland, Romania, Spain and Switzerland (Drury, et al., 2021). Notably, these studies looked at the use of vaccine passports not only for the mitigation of the spread of COVID-19, but for a range of different communicable diseases. The research mirrors the Canadian findings on attitudes towards the use of vaccine passports for international travel, in that public attitude was generally favourable. In contrast however, the research suggested that public opinion is unfavourable

towards their use in the context of access to work and other activities. A similar study from the UK observed similar attitude and studied the factors which act as predictors of acceptance of vaccine passports (Lewandowsky, Dennis, Kashima, White, & Garrett, 2021). This study found that greater trust in government, increasing age and greater perceived risk of the disease were associated with more favourable attitudes. The authors suggest that these findings suggests that the British public are willing, to an extent, to ‘trade-off’ between their privacy and the interests of public health. Significantly, the research also demonstrated that the specifics of the policy had a relatively insignificant impact on the level of public acceptance for a vaccine passport policy. The authors posited that although this “is surprising in light of people’s responses to opinion surveys which place a high value on privacy... . (is) consonant with the fact that people tend to reveal personal information for relatively small rewards, contrary to their stated opinion.” (Kokolakis, 2017)(Norberg, Horne, & Horne, 2007) (Wang, Duong, & Chen, 2016).

Trust among Vulnerable Populations

As highlighted through this literature review to this point, many studies have highlighted those levels of trust and acceptance in data sharing varies by demographic groups. For example, the Office of the Privacy Commissioner of Canada’s 2020-2021 Survey of Canadians on Privacy-Related Issues found that university educated (47%) and younger (52%) Canadians were more comfortable with government collection and use of data for public policy decisions.



The 2020-2021 Survey of Canadians on Privacy-Related Issues found that university-educated (47%) and younger (52%) Canadians were more comfortable with government collection and use of data for public policy decisions. These views were also more prominent among those from Ontario (47%), Atlantic Canada (43%) and Quebec (41%).

(Source: Office of the Privacy Commissioner of Canada, 2020-2021 Survey of Canadians on Privacy-Related Issues)

Figure 10: “I am comfortable with government collection and use of data for public policy decisions.”

These views were also more prominent among those from Ontario (47%), Atlantic Canada (43%) and Quebec (41%). Conversely, a study evaluating Canadians’ trust in genomic data sharing found several differences in levels of acceptance by age, finding that persons over the age of 60 had significantly higher levels of trust with the sharing of this data than did other age groups.

The research also reflects concern among the Canadian community that sharing of data could result in negative outcomes for already marginalised members of society. As highlighted by qualitative

research from British Columbia and Ontario, one of the primary hesitations for the collection and secondary use of health data is the potential for misuse or perpetuation of negative outcomes for already marginalised populations (Teng, Bentley, Burgess, O'Doherty, & McGrail, 2019) (Parica, Nunes du Melo, & Schull, 2019). The groups identified in this research include children, the elderly, as well as indigenous populations. Unfortunately, no research was identified through the course of this review which sought to quantify the relative levels of trust and acceptance of government data sharing among vulnerable and marginalised populations, including Indigenous persons and those who identify as LGBTQ2S+. However, recent research has examined the use of indigenous peoples' data during COVID-19 across international boundaries, including in Canada (Carroll, et al., 2021). This research found that that internationally, systemic policies and "historic and ongoing marginalization, have led to limitations in quality, quantity, access, and use of Indigenous Peoples' COVID-19 data."

Internationally, a number of systemic literature reviews which have identified varying levels of trust and acceptance of data sharing among different populations and demographic groups, and particularly those who are vulnerable or marginalised. One such study includes a systematic review and thematic synthesis of more than 25 studies conducted, predominantly in North America and the UK. The thematic analysis highlighted several demographic factors which reduced willingness to consent to sharing of health data. One such factor was a respondents' identified ethnicity (Hutrchings, Loomes, Butow, & Boyle, 2021). In the UK, white respondents were much less likely (59%) to consent to data sharing than non-white participants (72%). Similarly, in the UK and US, persons who identified their ethnicity as British/Irish white had higher consent compared to other groups. In the US, those who identified as African-American were also less likely to consent to data usage. Other factors which were associated with increased acceptance of data sharing were higher levels of education, gender (males were, in some instances, found to be more likely to consent to data sharing) and age, in that older participants were more willing to share or link data than younger populations.

'Privacy Calculus' a Contributing Factor to Public Acceptance of Data Sharing

As data collection and analysis technology has advanced over the past few decades, there has been an exploration into the factors which contribute to individuals' privacy concerns and acceptance of data use. One of the central theories used to understand the factors which influence individual's levels of acceptance on citizen privacy and data sharing is the Privacy Calculus Theory (PCT) (Wolfe & Laufer, 1977). The theory is based around the central idea that people's behaviour is based on a trade-off between the potential costs and benefits that the behaviour will create. As such, the PCT posits that individuals make privacy-related decisions to disclose and allow the sharing of personal information where they perceive that the positive benefits outweigh the negative outcomes of providing personal information. Research has demonstrated an extensive range of factors which

individuals use in their calculus of costs and benefits of an outcome. For example, negative impacts include what is referred to as 'risk beliefs', which research has shown include a sense of intrusion, surveillance and privacy concerns around health information. Positive outcomes relate to the perceived positive benefits of the technology in question, including health benefits and the perception of the benefits of government data collection and sharing (Dinev, 2014) (Fox, 2020). These theories have been supported in a range of contexts, including recently in the levels of public acceptance of COVID-19 contact tracing applications (Lewandowsky, Dennis, Kashima, White, & Garrett, 2021). Indeed, a recent study in this context concludes that people *"engage in a readily-understandable privacy calculus. Specifically, people trade off the perceived harms from the policy under consideration (tracking apps or immunity passports) against the perceived risk from COVID-19: increased risk perception increases policy acceptance and increased fear of fallout from the policies reduces support."*

Research Gaps

As highlighted by this review, the majority of literature related to the public's level of acceptance of data sharing relates to the collection and sharing of health-related data. Even prior to 2020, studies predominantly focused on levels of trust for the collection and sharing of health data, such as genomic and medical information. Interestingly, the need for tools such as contact tracing during the COVID-19 pandemic has led to an expansion of research on public acceptance in broader contexts, such as for the collection and sharing of location and administrative data. Nonetheless, at present, there remains a lack of research on levels of public acceptance of government data sharing for purposes outside the collection and sharing health data. This is true not only at a Canadian provincial and national level, but also at an international level. As such, there is a current gap in literature on levels of acceptance of data sharing for purposes such as on inter-governmental sharing of administrative data for improved delivery of social services. Similarly, there is a dearth of research examining whether levels of acceptance differs depending on which stakeholders will access to that data, and the association with the levels of trust in these stakeholders.

It is also notable that there is a lack of research on public acceptance of data sharing in a Canadian context overall, and particularly at a provincial level. For example, no Canadian research has been identified which specifically studies the levels of trust in government and associated levels of acceptance of inter-governmental sharing of data across Canada. As such, no research offers comprehensive insights into the potentially varied levels of trust and acceptance of data sharing across different segments of the Canadian population, such as differences across geographic regions or minority populations. This presents substantial challenges for policymakers in making decisions on data-sharing in a Canadian context, and particularly to ensure the safe and ethical sharing of data for marginalised and vulnerable populations. Understanding the nature of regional and urban-rural/small centres differences throughout Canada as well as age difference to fill these gaps will lead to a more comprehensive understanding of the public's acceptance of data sharing.



05.

Overview of Key Legislation

Overview of Key Legislation

The following summarizes key findings coming from a review of public and private sector legislation in Canada, and discussions with Information Privacy Commissioners, Government Information Access and Privacy Offices, and Chief Digital Officer's offices across Canada:

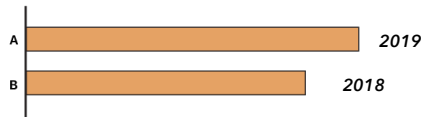
Key Insights

- The public is aware of the legislation governing privacy, the use of their information and feel that the federal government, in general, respects their privacy rights. Also, Canadians trust the private sector slightly more than government to protect against cybersecurity threats. *(Source: ICCS Citizens First Surveys from 2018 and 2020)*
- Themes that have emerged from the public include:
 - great concern regarding the use of Artificial Intelligence and facial recognition;
 - erosion of consent; and,
 - use of data for non-administrative purposes does not always align with existing legislation.
- To fully realize the benefits from the digital economy, numerous Canadian P/Ts have undertaken legislative reforms to:
 - drive innovation by opening up the silos of data between departments;
 - facilitate sharing of data to allow government to provide better services to citizens;
 - prevent citizens from having to share their PI multiple times; and,
 - make data available for driving decisions, where now they could become more politically motivated.
- There has been an increase in the introduction of private-sector privacy legislation in Canada.
- Political will, an embedded mandatory review of legislation and an active Information and Privacy Commissioner's office helped some jurisdictions achieve substantial changes to their public sector legislation.
- Many international jurisdictions (especially the United States) have, or are in the process of, enacting or making analogous changes to their privacy legislation.

Introduction

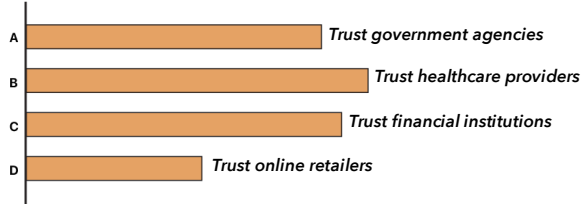
A review of the public and private sector legislation in Canada has shown that to fully benefit from the digital economy and share data for administrative and non-administrative purposes legislative reform is necessary. Political will, an embedded mandatory review of legislation and an active Information and Privacy Commissioner office helped some jurisdictions achieve substantial changes to their public sector legislation.

The public is aware of the legislation governing privacy, the use of their information and has a good level of trust in these.²³



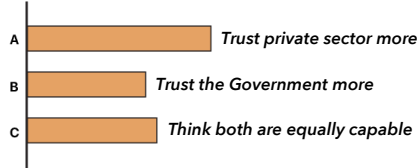
More than six in 10 Canadians (63%; up from 55% in 2018) feel that the federal government, in general, respects their privacy rights.

Figure 11: "I feel the federal government respects my privacy rights."



Close to six in ten (57%) citizens say they trust government agencies to keep personal information safe and secure. This is slightly lower than trust for healthcare providers (66%) or financial institutions (62%), but much higher than trust in online retailers like Amazon (37%).

Figure 12: "I trust certain organizations to keep my personal information safe."



Canadians trust the private sector (37%) slightly more than the government (25%) to protect against cybersecurity threats, while 23 per cent say both are equally capable.

Figure 13: Canadians' trust that private and public sector organizations will safeguard personal information.

(Source for all three figures: ICCS Citizens First Surveys from 2018 and 2020)

Approach

A legislative scan of Canadian Federal, Provincial, Territorial and Municipal (F/P/T/M) legislation was performed. This involved research on the use of data by F/P/T/M governments to improve service delivery and the level of acceptance by Canadians of these different uses and disclosures, including levels of public acceptance with the:

- sharing of personal information for administrative purposes;

²³ Source: ICCS Citizens First Surveys from 2018 and 2020

- use of service-related data and information for non-administrative purposes; and,
- types of data and personal information is currently shared, under what authorities and for what purposes.

A legislative scan of other jurisdictional approaches (specifically the US, UK, Estonia, and Australia) was also performed.

An analysis of the key international arrangements related to data privacy and data sharing (e.g., coming from the OECD and other international bodies) to which Canada subscribes was not included in the scope of this report. However, this analysis and an exploration of the linkages between this report and those international agreements would be germane to further discussions coming from this report, and could be included in a future phase of this work.

Interviews with Canadian Information and Privacy Commissioners (IPC), and Government Information Access and Privacy Offices

All Canadian Information and Privacy Commissioners (IPC), and P/T government Information Access and Privacy (IAP) offices were invited to participate. It was hoped this would provide a good cross-section of what information is collected by government, how it is used, stored, shared or deleted and the legislative regimes that support this. It was also believed that these entities would understand the public's perception of the government's use of their data.

Information and Privacy Commissioners/Ombudsman

A standard set of questions was prepared and used for all interviews.

The themes that emerged from these consultations showed:

- great concern regarding the use of Artificial Intelligence and facial recognition;
- erosion of consent; and,
- use of data for non-administrative purposes is against existing legislation.

Very few IPC offices do any proactive research on public perceptions and operate on a complaint-based process only.

Government IAP Offices

Generally, governments are not proactively seeking public perceptions on the use of data or trust of that process. There has been limited public engagement across Canada and it is generally issue or initiative specific.

The governments that responded or were consulted via survey identified a lack of resources or capacity and geographic challenges as the major stumbling blocks to conducting public engagement. Other comments that they shared included:

- legislative modifications were needed to drive innovation;
- frustrations within the creation of silos of data between departments;
- governments should be sharing PI and data better internally to provide better services to citizens;

- residents don't feel they should have to share their PI multiple times and prefer the government to find ways to integrate access to their PI; and,
- not enough data was available to drive decisions, so they were often politically motivated.

Web-based research of all Provinces and Territories and Federal legislation

This research focussed on the Federal, Provincial and Territorial (F/P/T) legislation and its impact on both public's trust and acceptance of data sharing.

More public consultation is happening slowly:

- Ontario has done extensive public engagement on its digital government and data strategies.²⁴
- Ministry of Service Alberta has launched an online consultation that will run until August 20, 2021, seeking stakeholder input on several privacy-related issues, including:
 - access to and control of one's personal information when interacting with government and private sector organizations.
 - the importance of clear and informed consent, data portability, and the right to be forgotten.
 - the need for greater transparency, such as plain language privacy statements.
 - the desire for legal requirements for collecting, using, and disclosing de-identified data.
 - enhancing government oversight to ensure public and private sector organizations protect personal information as new technologies emerge.

Survey of Chief Data or Information Officers

The consultations with Information and Privacy Commissioners and Government Information Access and Privacy Offices across Canada did not yield as many responses as were anticipated so a survey was devised and sent to the Chief Digital Officer (CDO) or Chief Information Officer (CIO) in select jurisdictions.

Overview of key legislation

An overview of key legislation governing the collection, use and disclosure of personal information across provinces, territories, and the federal government was conducted. Its purposes were to

²⁴Source: <https://www.ontario.ca/page/digital-and-data-strategy-consultations>
<https://www.ontario.ca/document/consultation-ontarios-digital-and-data-strategy>

identify key similarities and any notable differences in approaches, particularly in respect of the collection, use and disclosure to other jurisdictions or governments within Canada for the provision of services.

There are 41 separate statutes, each with its own regulations, addressing privacy at the Federal, and Provincial / Territorial (F/P/T) levels. Only three jurisdictions have distinct legislation for municipalities: Ontario, Saskatchewan, and Nova Scotia. All other municipalities fall under the respective provincial freedom of information and protection of privacy legislation.

Federal Acts

Canada has two federal laws which form the basis for data sharing across government. These two acts are the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*.

Personal Information Protection and Electronic Documents Act

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into force in 2000 and applies to the commercial transactions of organizations that operate in Canada's private sector.

More specifically, PIPEDA applies to organizations that are federally regulated and fall under the legislative authority of the Parliament of Canada, such as the telecommunications and broadcasting industry, and all local businesses in Yukon, Nunavut, and the Northwest Territories.

PIPEDA applies to the private sector of each province unless a province has enacted its own privacy legislation that is substantially similar to PIPEDA. Organizations subject to a substantially similar provincial privacy law are generally exempt from PIPEDA with concerning the collection, use or disclosure of personal information that occurs within that province. Currently, only Alberta, British Columbia and Québec have "substantially similar" privacy legislation in place.

PIPEDA continues to apply to federal works, undertakings or businesses that operate in those provinces as well as all interprovincial and international transactions by all organizations subject to PIPEDA during their commercial activities.

Organizations that operate interprovincially or internationally are required to deal with both provincial and federal privacy legislation.

The Privacy Act

The Privacy Act came into effect in 1983 and is the law governing the personal information handling practices of federal government institutions. This act applies to all personal information the federal government collects, uses and discloses regardless of if they are regular individuals or federal employees. This legislation applies directly to any federal body. The Act also gives people the right to access and request correction of personal information held by federal institutions.

Private Sector Legislation

There is an increase in the introduction of private-sector privacy legislation in Canada. As mentioned above, British Columbia, Alberta, and Quebec have their own private sector privacy legislation. These pieces of legislation have been deemed to be substantially similar to PIPEDA.

Ontario and Manitoba recently introduced their own private sector privacy law public consultations.

Key similarities in legislation

All access to information and protection of privacy laws in Canada protect and encompass the Model Code for the Protection of Personal Information developed by the Canadian Standards Association. The *CSA Model Code for the Protection of Personal Information* was developed by the Canadian Standards Association in 1996 with a 45-member committee composed of representatives from government, businesses, academics, consumers, and information technology and security experts.²⁵ These principles also formed the basis of PIPEDA, and are defined in Appendix D.

Canadian health care privacy legislation is comprised of 14 government jurisdictions (the Federal Government, 10 Provinces, and 3 Territories) each with its own legislative framework for protecting the privacy of personal information (PI), or personal health information (PHI).

All public sector access to information and protection of privacy laws (whether federal, provincial, or territorial) preserve a list of rights for the public²⁶. These rights include:

RIGHT OF ACCESS	Under Canadian Privacy Statutes, organizations must, upon request and subject to limited exemptions, inform individuals of the existence, use and disclosure of his or her personal information, and must give them access to that information, including a listing of the third-party organizations with whom the information has been shared.
RECTIFICATION OF ERRORS	Canadian privacy statutes generally require that when an individual demonstrates the inaccuracy or incompleteness of his or her personal information held by an organisation, the organisation must correct the inaccuracies and/or add a notation to the information, as appropriate.
DELETION/RIGHT TO BE FORGOTTEN	While Canadian provincial / territorial (P/T) Privacy Statutes afford individuals the right to withdraw consent and challenge the accuracy, completeness, and currency of their personal data, they do not grant a

²⁵ Source: <https://www.privacysense.net/10-privacy-principles-of-pipeda/>

²⁶ Adapted from <https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf>

	specific right to require organizations to “erase” or delete their personal information per se. (While not a specific right, privacy regulations do allow for the early disposal of personal information in certain circumstances.)
OBJECT/RESTRICT PROCESSING	Individuals give consent to the use or disclosure of their personal information beyond that which is required to fulfil the explicitly specified and legitimate purpose for its collection. Also, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Upon receipt of any withdrawal, individuals must be informed of the implications of such withdrawal.
DATA PORTABILITY	Although Canadian Privacy Statutes include a right of access to personal information (see above), they do not include a right to data portability.
WITHDRAW CONSENT	Under Canadian P/T Privacy Statutes, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Individuals must be informed of the implications of such withdrawal.
OBJECT TO MARKETING	Consent is required for the use or disclosure of personal information for marketing purposes. The form of consent required (opt-in or opt-out) will vary depending on the circumstances, the sensitivity of the information and the reasonable expectations of the individual.
COMPLAIN TO THE RELEVANT DATA PROTECTION AUTHORITY(IES)	Individuals have a right to make a complaint to the relevant data protection authority. At the provincial and territorial level, organizations must have easy-to-access and simple-to-use procedures in place to respond to complaints or inquiries and must take steps to effectively address complaints accordingly.

Authority(ies) responsible for data protection

Each Canadian jurisdiction - federally, provincially, and territorially - has its own independent Information and Privacy Commissioner or Ombudsman who reports to their respective legislature and oversees the relevant data protection laws applicable in that jurisdiction.

Insights & Notable differences for sharing with other jurisdictions or governments within Canada

When differences were found they were based on the premise that an individual owns the information about them. Political will, an embedded mandatory review of legislation and an active IPC office helped some jurisdictions achieve substantial changes to their public sector legislation.

Several changes have happened in Canada regarding updating and amending existing legislation that did not allow for the sharing of data for non-administrative purposes.



British Columbia

In British Columbia, a special committee ²⁷ of the Legislative Assembly has been established to review the Personal Information Protection Act, consider input on it and issue reports. This committee is facilitating discussions for considering amendments to PIPA, and some of the issues include:

- mandatory breach reporting;
- consents; and
- making PIPA substantially like federal legislation (i.e. PIPEDA).

They are also conducting public consultations in a variety of ways (public and online consultations) to advance their indigenous data sovereignty initiatives.

Declaration Act

The provincial government passed the Declaration on the Rights of Indigenous Peoples Act (Declaration Act) into law in November 2019. The Declaration Act establishes the UN Declaration as the Province's framework for reconciliation, as called for by the Truth Reconciliation Commission's Calls to Action. This historic legislation was developed in collaboration and consultation with Indigenous partners. B.C. is the first province or territory in Canada to pass legislation to implement the UN Declaration - recognizing in law the human rights of Indigenous peoples.

The Declaration Act aims to create a path forward that respects the human rights of Indigenous peoples while introducing better transparency and predictability in the work government shares with them. It requires development of an action plan to achieve this alignment over time - providing transparency and accountability. the objectives of the UN Declaration. And it requires regular annual reporting on progress to the Legislature, providing transparency and accountability. to monitor progress.

In addition, the legislation allows for flexibility for the Province to enter into agreements with a broader range of Indigenous governments, and it provides a framework for decision-making between Indigenous governments and the Province on matters that impact their citizens.

²⁷ More information about the Special Committee can be found here: <https://www.leg.bc.ca/parliamentary-business/committees/42ndParliament-2ndSession-pipa>



Manitoba

On November 2, 2020, the government in Manitoba introduced Bill 49, an Act to amend The Freedom of Information and Protection of Privacy Amendment Act. Public bodies are permitted to disclose personal information to deliver common or integrated services on specified conditions and permitted to disclose personal information to evaluate or monitor their programs, or to carry out research and planning relating to them.

The government of Manitoba also introduced Bill 54, An Act to Amend the Personal Health Information Amendment Act and two applicable features are that a trustee can use personal health information while educating employees, agents, students, and health professionals to provide health care.



Northwest Territories

The amended ATIPP Act for the Northwest Territories came into effect on July 30, 2021. The Act will now provide improved public accountability through access to government information, as well as more safeguards for how personal information is collected, used, and disclosed by public bodies.



Newfoundland

Newfoundland has amended its ATIPP legislation twice since 2011 to allow for easier and more secure administrative and non-administrative uses of data throughout all of government.



Ontario

The Ontario Government has introduced a white paper explaining new private sector privacy legislation for businesses and the non-government sector.



Quebec

In June 2020, the government of Quebec introduced Bill 64, *An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information*. Features include:

- amends the Act respecting the protection of personal information in the private sector to create the function of a person in charge of the protection of personal information within enterprises and to require enterprises to ensure that the parameters of the technological products or services they use to collect personal information provide the highest level of confidentiality by default, without any intervention by the person concerned.

- the Bill requires public bodies and enterprises to provide certain information to the person concerned when they collect personal information using technology that includes functions allowing the person to be identified, located, or profiled, or when they use personal information to render a decision based exclusively on automated processing of such information. It establishes a person's right to access computerized personal information concerning him or her in a structured, commonly used technological format or to require such information to be released to a third person.

On June 9th, 2021, Bill 95 - "An Act to amend the Act respecting the governance and management of the information resources of public bodies and government enterprises and other legislative provisions" was adopted. This Act establishes a new framework for the management of government digital data held by public bodies, and will require government departments and agencies to plan and undertake initiatives to digitize the personal information of the citizens of Quebec. The law also strives to streamline the sharing of digitized personal information within government.



The Yukon Legislative Assembly has passed the new Access to Information and Protection of Privacy Act, Bill 24, which came into force on April 1, 2021. Features of the Act include:

- replacing the existing Act's record-based approach with a new information-based approach.
- establishing three prescriptive categories of public bodies and prescribed entities.
- entrenching privacy-by-design principles in the carrying out, or provision of, programs activities and services by ministerial bodies through requiring those bodies to conduct privacy impact assessments in certain cases.
- enabling public bodies to:
 - provide integrated services in collaboration with partner agencies;
 - provide a government-wide personal identity service; and,
 - carry out data-linking activities.

International Best Practices



Data Availability and Transparency Act

Australia has drafted but not enacted its Data Availability and Transparency Act. There were many difficulties sharing data under its Privacy Act drafted in the 1980's. This new Act authorizes public sector data custodians to share data with accredited users in accordance with specific authorizations, purposes, principles, and agreements.

Consumer Data Rights Act (CDR)

CDR will give consumers greater access to and control over their data and will improve consumers' ability to compare and switch between products and services.

Under the CDR, AU residents can direct that their data to be shared via a secure online system with an accredited provider of their choice.



Estonian personal data protection originates from the 1996 Personal Data Protection Act (PDA). The PDPA has adapted over time to reflect changing technologies and practice, one central component has remained the same: consent.

Sensitive personal information (biometric, ethnicity, sex life, trade union membership, state of health, for example) can only be opened by a government agency if the subject willfully consents to its usage. To elaborate further, the PDPA does not consider "silence or inactivity" consent and gives citizens the right to make consent "partial and conditional". By expanding the concept of consent, Estonian citizens are protected against their personal information being processed without permission. It also lets citizens flexibly choose which e-service fits their needs most.

Estonia is on the leading edge for shared information with its X Road System and over 3,000 public and private entities use the system, performing over 1.3 billion transactions annually



The UK Digital Identity and Attributes Trust Framework, which is similar to Canada's Pan-Canadian Trust Framework, was introduced in July of this year. The framework shows how organisations can be certified to provide secure digital identity services; they will have to go through an assessment process with an independent certification body. It also states how data can be shared between organisations and announces the government will start testing the framework in partnership with service providers. Following consultation with a range of public and private organisations last year, the Government has produced a draft (or 'Alpha') version of the document, which it has invited organisations and citizens to comment on.

United States of America

There have been significant data privacy developments from 2020 in the United States:



The *California Consumer Privacy Act (CCPA)* went into effect this year, giving Californian consumers the right to take more control over their data.

This landmark law secures new privacy rights for California consumers, including the right to:

- know about the personal information a business collects about them and how it is used and shared.
- the right to delete personal information collected from them (with some exceptions).
- the right to opt-out of the sale of their personal information; and
- the right to non-discrimination for exercising their CCPA rights.

The *California Privacy Rights Act (CPRA)* works as an addendum to the CCPA - strengthening rights of California residents, tightening business regulations on the use of personal information (PI), and establishing a new government agency for state-wide data privacy enforcement called the California Privacy Protection Agency (CPPA).

The *CPRA* becomes fully effective on January 1, 2023. Enforcement is scheduled to begin on July 1, 2023 - with a so-called lookback period to January 1, 2022, meaning data collected from that date on is liable for compliance.



Delaware

On January 1, 2016, the Delaware Online Privacy and Protection Act (“DOPPA”) went into force. This is a law that provides strong online privacy protection for its residents, including one that requires the state government to get rid of consumer data after a set period of time.



Connecticut

Connecticut's Insurance Data Security Law went into effect on October 1, 2020. The Act establishes standards applicable to licensees of the Connecticut Insurance Department for data security, the investigation of a cybersecurity event, and notification to the Department of such event.



Nevada

Nevada was the first state to provide consumers with the right to opt out of the sale of their personal information under its Senate Bill 220 in October of 2019. Senate Bill 220 requires companies to honor consumers' requests to no longer sell their data within 60 days. The Nevada Attorney General can bring legal action against companies in violation of the bill, as well as issue fines up to \$5,000 per violation. Companies are still allowed to share personally identifiable information with their own business affiliates and, for an individual to be eligible to opt-out, a business must intend to sell the data.



New York

A proposed amendment to New York's Civil Rights Law would create criminal liability for certain privacy violations, and the proposed It's Your Data Act would create CCPA-like consumer privacy rights but with a broader private right of action.

The New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which amended New York's breach notification law and required covered businesses to implement and maintain reasonable security measures, went into effect in March 2020.



Oregon

Oregon lacks comprehensive data privacy legislation but enshrines privacy protections with a combination of common law torts, such as invasion of privacy, and sector-specific laws. Oregon updated its data breach notification law in 2019, which has now become the Oregon Consumer Protection Act.



Virginia

The passage of the Virginia Consumer Data Protection Act (CDPA) earlier this year will offer a range of new rights to the residents of the Old Dominion. Like the California Consumer Privacy Act, the CDPA includes a clear threshold where businesses are covered if they process the personal data of:

- 100,000 Virginia residents on an annual basis, or
- 25,000 Virginia residents on an annual basis and over fifty percent of their gross revenue is derived from the sale of personal data.

The CDPA will apply as of January 1, 2023.



Washington

The Senate Bill 5062, the Washington Privacy Act has had a bumpy road to acceptance. For three consecutive years its legislators attempted to pass it and it failed because they couldn't to agree on an enforcement mechanism.



06.

Recommendations

Recommendations

Based upon the research presented, there are eight recommendations for the ICCS Joint Councils to consider as next steps for advancing upon the findings from this report. The recommendations have been organized into three themes, including:

Theme 1: Understanding levels of public trust

- **Recommendation A:** Engage with the public across Canada to better understand their levels of acceptance of government data use.
- **Recommendation B:** Encourage governments to establish formal and ongoing monitoring of Canadians' levels of public acceptance of data use and sharing (with a focus on identifying differences in levels of acceptance across different geographic regions, urban-rural/small centres, and demographic groups).

Theme 2: Strengthening the relationship between government and the public






- **Recommendation C:** Support government to take specific actions to promote transparency to build or regain trust.
- **Recommendation D:** Encourage governments to allow citizens to opt into a “tell us once” approach, where data may be shared with other government departments for a set of agreed uses, in alignment with public sector legislative contexts within Canada.
- **Recommendation E:** Advocate for the prioritization of Indigenous Data Sovereignty by government organizations.










Theme 3: Improving internal government operations




- **Recommendation F:** Encourage governments to establish centralized Data Authorities, in alignment with public sector legislative contexts within Canada.
- **Recommendation G:** Educate public servants on what information they can and cannot share (secondary usage) and the requirements for consent, according to privacy legislation in their jurisdiction.
- **Recommendation H:** Encourage and support F/P/T/M legislative reform to enable the secondary uses of data not currently allowed.










An estimated *level of complexity* and *implementation effort* has been assigned to each of the eight recommendations, along with a suggested range of specific activities that could be undertaken to move them forward. With the exception of Recommendation A, which can be led








and implemented entirely by ICCS, our estimation of the complexity and effort level relates to what will be required from government organizations to complete a given recommendation.

				
Recommendation		Suggested Activities	Complexity	Effort
<p>A Engage with the public across Canada to better understand their levels of acceptance of government data use</p>	<ul style="list-style-type: none"> a. Conduct public consultation to develop an understanding of the levels of acceptance, as well as the key factors and/or events which have shaped these attitudes b. Validate any insights against the findings of this report c. When conducting public consultation: <ul style="list-style-type: none"> i. Identify and be clear about reasons for/goal of engaging with the public ii. Ensure a mix of short survey-style engagement and in-depth discussion-based consultation iii. Ensure that in the collection of this data, the sample population is representative and captures differences across geographic regions and demographic groups (particularly vulnerable populations) 			
<p>B Encourage governments to establish formal monitoring of Canadians' levels of public acceptance of data use and sharing (with a focus on identifying differences in levels of acceptance across different geographic regions, urban-rural/small centres, and demographic groups)</p>	<ul style="list-style-type: none"> a. Promote the collection of a longitudinal survey dataset on Canadians' attitudes towards the use and sharing of data b. Share best practices from jurisdictions that are starting (e.g., British Columbia, Alberta, Ontario) or are already doing this (e.g., New Zealand and the Kiwis Count quarterly public survey) c. Ensure that in the collection of this data, the sample population is representative and captures differences across geographic regions and demographic groups (particularly vulnerable populations) d. Document acceptance of intended data use (e.g., health, intelligence collection, broad, etc.), as well as public acceptance as a whole 			

				 High	 Medium-High	 Medium	 Medium-Low	 Low	
Recommendation	Suggested Activities	Complexity	Effort						
C	<i>Support government to take specific actions to promote transparency to build or regain trust</i>	<ul style="list-style-type: none"> a. Encourage government to continue to be consistently transparent about why it is collecting public information, what it will be used for, who it might be shared with, and the authority under which it is being collected b. Encourage government to leverage research on the factors, events and purposes which build and diminish trust in data sharing, including fostering open data, to inform the development of data sharing policies for which there is existing public support c. Encourage government to prioritize and continuously improve systems that support the accuracy, completeness, and reliability of data, and data protection d. Support government in highlighting programs and policies which have successfully shared data to provide high-quality services to constituents across platforms and geographies e. Engage with international geographies which have undertaken research and knowledge sharing initiatives in their respective regions, including Australia, the United Kingdom, and the United States f. Analyze results from public consultations (Recommendation A) and generate a report to highlight ways that governments can enhance transparency and value in their use of citizen data 							
D	<i>Encourage governments to allow citizens to opt into a “tell us once” approach, where data may be shared with other government departments for a set of agreed uses, in alignment with public sector legislative contexts within Canada</i>	<ul style="list-style-type: none"> a. Share best practices from jurisdictions that are already doing this, such as Australia b. Encourage Canadian P/T/M governments to engage in international knowledge sharing opportunities and groups to leverage lessons learned across other jurisdictions, including engagement with existing international knowledge sharing groups 							

				
Recommendation		Suggested Activities	Complexity	Effort
		<ul style="list-style-type: none"> c. Support governments to leverage existing research and expertise to ensure that implemented programs: <ul style="list-style-type: none"> i. Allow citizens to opt-in or out ii. Ensure accessibility for low-tech users iii. Ensure the user feels their information is private and secure iv. Follow the guidelines available on meaningful consent from IPC Canada 		
E	<i>Advocate for the prioritization of Indigenous Data Sovereignty by government organizations</i>	<ul style="list-style-type: none"> a. Engage with community to understand the Indigenous perspective on data sovereignty through inclusive, robust consultation, and provide this information to government (this may be progressed alongside or as part of Recommendation B) b. Ensure that consultation is community-driven and Nation-based c. Encourage governments foster meaningful collaboration and reciprocal partnerships with Indigenous communities d. Share best practices from jurisdictions that are already doing this, such as British Columbia e. Promote government uptake of a Data Authority that follows the First Nations Information Governance Centre guidelines to oversee data collection and use, as is being done in Ontario f. Seek international perspectives from countries such as New Zealand and Australia on key considerations to effectively engage on data sovereignty for data sharing initiatives 		

				 High	 Medium-High	 Medium	 Medium-Low	 Low
Recommendation	Suggested Activities	Complexity	Effort					
F <i>Encourage governments to establish centralized Data Authorities, in alignment with public sector legislative contexts within Canada</i>	<ul style="list-style-type: none"> a. Encourage all governments to establish a clearly defined role (e.g., Digital Officer) with a centralized mandate to lead the following activities, amongst others: <ul style="list-style-type: none"> i. Update policies and develop data sharing protocols to facilitate sharing of data within government to enable enhanced service delivery ii. Foster awareness / knowledge of legislation regarding what data can be shared for secondary uses and what cannot iii. Work with CIOs to ensure data is secure and in a user-ready state iv. Supporting best practice in data sharing to ensure the user feels their information is private and secure b. Leverage learnings and best practices from jurisdictions that already have this role in place – such as from Ontario, British Columbia and Prince Edward Island 							
G <i>Educate public servants on what information they can and cannot share (secondary usage) and the requirements for consent, according to privacy legislation in their jurisdiction</i>	<ul style="list-style-type: none"> a. Create, or support governments to create, training programs that address learning gaps (ensure training includes refresher sessions) b. Update (or support governments to update) training and learning materials to reflect both current practices and orders / recommendations from IAP or IPC c. Encourage governments to make privacy policies and procedures easily accessible d. Educate staff on the concepts of <i>Open by Design</i> and <i>Security by Design</i>, and on how adopting them could help to build public trust in government’s data collection and use 							

				 High	 Medium-High	 Medium	 Medium-Low	 Low
Recommendation	Suggested Activities	Complexity	Effort					
H <i>Encourage and support F/P/T/M legislative reform to enable the secondary uses of data not currently allowed</i>	<ul style="list-style-type: none"> a. Encourage governments to reach out to jurisdictions identified in Section 06. Overview of Key Legislation to learn about their approach to legislative reform, and to identify alignment with any desired legislative reforms b. Facilitate discussions with governments to help them understand where they would want to pursue secondary uses of data. c. Encourage governments to consider amending legislation to better support evolving government practices and citizens' expectations, including changes that would facilitate easier sharing of personal information between entities within government, and also with approved external entities. d. Encourage governments to enhance their emphasis on protection of personal information through changes to legislation and regulations. e. Encourage governments to harmonize laws to enable better and more efficient sharing of information across governments and across borders - including internationally. 							

Observations

Key observations relating to the guide are included below:

1. Recommendation A is high priority, relatively low complexity and effort, and within the control of the ICCS. We recommend that this is sequenced first.
2. Recommendations B through H involve influencing governments to take action. As such, we recommend that they are undertaken in parallel. This will help to streamline communications from government's perspective and optimize resourcing for the ICCS.
3. Recommendation H is a key input to Recommendation D, as legislative change would better equip governments to offer a "tell us once" approach, where data can be shared across departments. Regardless, the advocacy component of Recommendation H can be progressed alongside Recommendation D.



07. Appendices

Appendix A: Sources for Literature Review

The following sources provided information for the completion of the Literature Review:

- Carroll, S. R., Akee, R., Chung, P., Cormack, D. C., Kukutai, T., Lovett, R., . . . Rowe, R. K. (2021). Indigenous Peoples' Data During COVID-19: From External to Internal. *Frontiers in Sociology, 6*.
- Dinev, T. (2014). Why Would We Care About Privacy. *European Journal of Information Systems, 23*, 97-102.
- Drury, J., Mao, G., John, A., Kamal, A., Rubin, J. G., Stott, C., . . . Marteau, T. M. (2021). Behavioural responses to COVID-19 health certification: a rapid review. *BMC Public Health(21)*.
- Dye, C., & Mills, M. C. (2021). COVID-19 vaccination passports. *Science, 371*, 1184.
- Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*.
- Fox, G. (2020). To protect my health or my privacy? A mixed methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology, 1-15*.
- Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behaviour, 121*.
- French, M., & Monahan, T. (2020). Dis-ease surveillance: How might surveillance studies address COVID-19? *Surveillance & Society, 18*.
- Garrison, N. A., Sathe, N. A., Matheny, A. H., Holm, I. A., Sanderson, S. C., Smith, M. E., . . . Clayton, E. W. (2016). A systematic literature review of individuals' perspectives on broad consent and data sharing in the United States. *Genetics in Medicine, 18*, 663-671.
- Ghafur, S., Van Dael, J., Leis, M., Darzi, A., & Aziz, S. (2020). Public perceptions on data sharing: key insights from the UK and the USA. *The Lancet: Digital Health*.
- Gostin, L. O., Halabi, S. F., & Wilson, K. (2018). Health Data and Privacy in the Digital Era. *JAMA, 320*, 233-234.
- Guillon, M., & Kergall, P. (2020). Attitudes and opinions on quarantine and support for a contact-tracing application in France during the COVID-19 outbreak. *Public Health, 21-31*.
- Hutchings, E., Loomes, M., Butow, P., & Boyle, F. (2021). A systematic literature review of attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on consent. *Systematic Reviews, 132*.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

- Lewandowsky, S., Dennis, S., Kashima, Y., White, J. P., & Garrett, P. (2021). Public acceptance of privacy-encroaching policies to address the COVID-19 pandemic in the United Kingdom. *PLoS ONE*, *16*.
- Middleton, A., Milne, R., Almarri, A., Anwer, Atutornu, J., Baranova, E. E., . . . Critchley, C. (2020). Global Public Perception of Genomic Data Sharing: What Shapes the Willingness to Donate DNA and Health Data? *The American Journal of Human Genetics*, *107*, 723-752.
- Milne, R., Morley, K. I., Howard, H., Niemiec, E., Nicol, D., Chritchley, C., . . . Middleton, A. (2019). Trust in genomic data sharing among members of the general public in the UK, USA, Canada and Australia. *Human Genetics*, *138*, 1237-1246.
- Munzert, S., Selb, P., Gohdes, A., Stoetzer, L. F., & Lowe, W. (2021). Tracking and Promoting the Usage of COVID-19 Contact Tracing App. *Nature Human Behaviour*, *5*, 247-255.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*, 100-126.
- Office of the Privacy Commissioner of Canada. (2021). *2020-21 Survey of Canadians on Privacy-Related Issues*. Gatineau: Office of the Privacy Commissioner of Canada.
- Ong, E., & Ling Loo, W. (2021). *Gauging the Acceptance of Contact Tracing Technology: An Empirical Study of Singapore Residents' Concerns and Trust in Information Sharing*. Singapore: Regulatory Insights on Artificial Intelligence: Research for Policy 2021.
- Open Data Institute. (2018). *Attitudes towards data sharing - Europe*. Open Data Institute.
- Pagliari, C., Davidson, S., Cunningham-Burley, S., Laurie, G., Mhariri, A., & Sethi, N. (2013). *Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes..* The Scottish Government.
- Parica, A., Nunes du Melo, M., & Schull, M. J. (2019). Social licence and the general public's attitudes toward research based on linked administrative health data: a qualitative study. *CMAJ Open*.
- Richter, G., Krawczak, M., Lieb, W., Wolff, L., Schreiber, S., & Buyx, A. (2017). Broad consent for health care-embedded biobanking: understanding and reasons to donate in a large patient sample. *Genetics in Medicine*, *76-82*.
- Saskia C. Sanderson, K. B. (2017). Public Attitudes toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US. *The American Journal of Human Genetics*, *414-427*.
- Savic-Kaltescoe, S., Middleton, A., & Milne, R. (2021). Public Trust and Genomic Medicine in Canada and the UK. *Wellcome Open Research*, *6*, 124.
- Schlagenhauf, P., Patel, D., Rodriguez-Morales, A., Gautret, P., & Grobusch, M. (2021). Variants, vaccines and vaccination passports: Challenges and chances for travel medicine in 2021. *Travel Medicine Infectious Disease*, *40*.

- Simpson, S. (2021). *Majority of Canadians Support Vaccine Passports for Variety of Indoor and Outdoor Activities*. Toronto: Ipsos Public Affairs.
- Teng, J., Bentley, C., Burgess, M. M., O'Doherty, K. C., & McGrail, K. M. (2019). Sharing linked data sets for research: results from a deliberative public engagement event in British Columbia, Canada. *International Journal of Population Data Science*, 4(1).
- Thompson, N., McGill, T., Bunn, A., & Alexander, R. (2020). Cultural Factors and the Role of Privacy Concerns in Acceptance of Government Surveillance. *Journal of the Association for Information and Science Technology*, 1129-1142.
- Tindana, P., & de Vries, J. (2016). Broad Consent for Genomic Research and Biobanking: Perspectives from Low- and Middle-Income Countries. *Annual Review of Genomics and Human Genetics*, 17, 375-393.
- Wang, T., Duong, T. D., & Chen, C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 531-542.
- Wolfe, M., & Laufer, R. S. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, 33, 22-42.
- Yasaka, T. M., Lhrich, B. M., & Sahyouni, R. (2020). Peer-to-peer contact tracing: A privacy-preserving smartphone application. *Journal of Medical Internet Research*, 8(4).
- Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs☆. *Information & Management*, 56, 570-601.

Appendix B: Jurisdictions Contacted for the Geographic Insights Scan

The following jurisdictions were engaged during the completion of the Geographic Insights Scan section of this report:

Juris.	Source Dept. / Org.
AB	<ul style="list-style-type: none"> FOIP and Information Management
BC	<ul style="list-style-type: none"> Citizens Services CDO Maple Ridge Municipal Government
MB	<ul style="list-style-type: none"> Information and Privacy Secretariat IPC
NB	<ul style="list-style-type: none"> Finance and Treasury Board CDO
NL	<ul style="list-style-type: none"> Access to Information and Protection of Privacy Office, Department of Justice and Public Safety CDO IPC
NS	<ul style="list-style-type: none"> Information Access and Privacy Unit
NT	<ul style="list-style-type: none"> Access and Privacy Office, Policy and Planning Division, Department of Justice IPC
NU	<ul style="list-style-type: none"> ATIPP Office, Department of Executive and Intergovernmental Affairs IPC
ON	<ul style="list-style-type: none"> Government and Consumer Services, Information Privacy and Archives Division CDO IPC
PEI	<ul style="list-style-type: none"> IT Security IPC
SK	<ul style="list-style-type: none"> Access and Privacy Branch, Ministry of Justice CDO
YT	<ul style="list-style-type: none"> ATIP Office, Department of Justice

Appendix C: Sources for Geographic Insights Scan

The following sources provided information for the completion of the Geographic Insights Scan:

- 2020-21 Survey of Canadians on Privacy-Related Issues - https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/
- *Annual Reports of Provincial and Territorial Information and Privacy Commissioners*
- Bloomberg Philanthropies - <https://www.bloomberg.org/>
- Building Trust: Lessons from Canada's Approach to Digital Identity Observer Research Foundation Issue Brief 2020 - <https://www.orfonline.org/research/building-trust-lessons-from-canadas-approach-to-digital-identity-67360/>
- Canadian Digital Identity Research 2020 Report - <https://diacc.ca/wp-content/uploads/2021/03/Canadian-Digital-Identity-Research-2020-Report-ENG-VF.pdf>
- Citizens First Surveys from 2018 and 2020 from ICCS - <https://citizenfirst.ca/research-and-publications/citizens-first/citizens-first-2020>
- Closing the Data Gap: How Cities Are Delivering Better Results for Residents A Monitor Institute by Deloitte report, in collaboration with What Works Cities June 2021 - <https://www2.deloitte.com/us/en/blog/monitor-institute-blog/2021/closing-the-data-gap.html>
- Data Advisory Board and Data Leaders Network - [https://www.gov.uk/government/groups/data-advisory-board-and-data-leadersnetwork#:~:text=The%20use%20of%20data%20in,Media%20%26%20Sports%20\(DCMS\).](https://www.gov.uk/government/groups/data-advisory-board-and-data-leadersnetwork#:~:text=The%20use%20of%20data%20in,Media%20%26%20Sports%20(DCMS).)
- Digital Identity: Focus on the Pan-Canadian Trust Framework JOINT COUNCIL'S EXECUTIVE MONTHLY REPORT (Product of the Research Committee) May 2020 - <https://citizenfirst.ca/assets/uploads/research-repository/Joint-Councils-Executive-Report-May-2020.pdf>
- It's Not Only Size That Matters: Trust and E-Government Success in Europe - <https://www.google.com/search?q=estonia+and+trust+in+government&oq=estonia&aqs=chrome.2.69i57j46i20i263i275i433i512j35i39l2j69i59j0i20i263i512j0i433i512j0i512l2j46i512.2425j0j15&sourceid=chrome&ie=UTF-8>
- Stats NZ - <https://www.stats.govt.nz/corporate/public-attitudes-to-data-integration>

- <https://www.stats.govt.nz/corporate/a-social-licence-approach-to-trust>
- New Zealand Government Kiwis Count Survey
<https://publicservice.govt.nz/our-work/kiwis-count-survey/>
 - Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service - <https://www.canada.ca/en/privy-council/corporate/clerk/publications/data-strategy.html>
 - Republic of Estonia Information System Authority - <https://www.ria.ee/en.html>
 - The Opioid Crisis and Response: Update to Council and Senior Administration, City of Calgary, June 21, 2018 - <https://www.calgary.ca/csps/cns/mental-health-and-addiction.html>
 - The Treasury Board Directive on Automated Decision Making - <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>
 - Trusted Digital Transformation Considerations for Canadian Public Policy January 2019) - <https://www.gov.uk/government/groups/data-advisory-board-and-data-leaders-network>
 - UK Digital Identity and Attributes Trust Framework - <https://www.gov.uk/government/news/next-step-in-plans-to-govern-use-of-digital-identities-revealed--2>

Appendix D: CSA Model Code

The following are the 10 principles that form the foundation of the CSA Model Code.

Accountability

An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

Identifying purposes

The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.

Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Limiting collection

The collection of personal information must be limited to that which is needed for the purposes identified by the organization. The information must be collected by fair and lawful means.

Limiting use, disclosure, and retention

Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept if required to serve those purposes.

Accuracy

Personal information must be as accurate, complete, and up to date as possible to properly satisfy the purposes for which it is to be used.

Safeguards

Personal information must be protected by appropriate security relative to the sensitivity of the information.

Openness

An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Individual access

Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to

challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging compliance

An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.

Appendix E: Sources for Overview of Key Legislation

The following sources provided information for the completion of the Overview of Key Legislation:

Consultations with:

- Federal, Provincial and Territorial Access to Information and Protection of Privacy Offices
- Federal, Provincial and Territorial Information and Privacy Commissioners / Ombudsman
- Office of Chief Digital Officers / CIO

Research Sources:

Office of the Privacy Commissioner of Canada

- **Jurisdictional Comparison: Privacy Protections 2020**
<https://www.priv.gc.ca/media/5434/jurisdictionalcomparison-eng.pdf>
- **2020-21 Survey of Canadians on Privacy-Related Issues**
https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca
- **Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service**
<https://www.canada.ca/en/privy-council/corporate/clerk/publications/data-strategy.html>

Treasury Board of Canada

- **Digital Operations Strategic Plan: 2018-2022**
<https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/digital-operations-strategic-plan-2018-2022.html>
- **Policy on Service and Digital**
<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603>
- **Policy on Privacy Protection**
<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510>
- **Canada's Digital Government Strategy**
The International Comparative Legal Guide to: Data Protection 2018 A practical cross-border insight into data protection law, Published by Global Legal Group, 5th Edition 2018
<https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf>

- **Guidance on Preparing Information Sharing Agreements Involving Personal Information**

<https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html>

Appendix F: Summary of Canadian Privacy Legislation

The following is a summary, by jurisdiction, of amendments made to legislation and their purpose.

Jurisdiction	Legislation Enacted	Amended and For What Purpose
AB	<p><u>PUBLIC SECTOR</u></p> <ul style="list-style-type: none"> Freedom of Information and Protection of Privacy Act (FOIP Act) 1995 Health Information Act 2001 <p><u>PRIVATE SECTOR</u></p> <ul style="list-style-type: none"> Personal Information Protection Act 2004 	<p>Alberta is the latest Canadian province considering public and private sector privacy law reforms, as the government of Alberta has initiated an online survey to collect feedback on the protections offered by the <i>Personal Information and Protection Act and the Freedom of Information and Protection of Privacy Act</i>.</p>
BC	<p><u>PUBLIC SECTOR</u></p> <ul style="list-style-type: none"> Freedom of Information and Protection of Privacy Act (FOIPPA) 1996 E-Health (Personal Health Information Access and Protection of Privacy Act 2008 <p><u>PRIVATE SECTOR</u></p> <ul style="list-style-type: none"> Personal Information Protection Act (PIPA) 2004 	<p>A special committee of the Legislative Assembly is considering amendments to PIPA.</p>
MB	<ul style="list-style-type: none"> Freedom of Information and Protection of Privacy Act (FIPPA) 1998 Personal Health Information Act (PHIA) 1997 	<p>Last amended January 2011</p> <p>Public bodies are permitted to disclose personal information for the purpose of delivering common or integrated services on specified conditions, to evaluate or monitor their programs, or to carry out research and planning relating to them.</p> <p>The government of Manitoba introduced Bill 54, an <i>Act to amend The Personal Health Information Amendment Act</i> but it has not passed yet.</p>

Jurisdiction	Legislation Enacted	Amended and For What Purpose
		On November 2, 2020, the government in Manitoba introduced Bill 49, an Act to amend <i>The Freedom of Information and Protection of Privacy Amendment Act</i> .
NB	<ul style="list-style-type: none"> • Right to Information and Protection of Privacy Act 2009 • Personal Health Information Privacy and Access Act 2009 	No amendments.
NL	<ul style="list-style-type: none"> • Access to Information and Protection of Privacy Act 2005 • Personal Health Information Act (PHIA) 2008 	<p>Last amended in 2012</p> <p>Defines “common or integrated program or service”, and “automated decision system”.</p> <p>Also defines “algorithmic impact assessments” and requires that any public body planning to implement an automated decision system complete one and, if requested, provide it to the Information and Privacy Commissioner.</p> <p>Requires public bodies to keep records of the decision-making processes of automated decision systems.</p>
NS	<ul style="list-style-type: none"> • Freedom of Information and Protection of Privacy Act (FOIPOP) 1993 • Personal Health Information Act (PHIA) 	No amendments.
NT	<ul style="list-style-type: none"> • Access to Information and Protection of Privacy Act (ATIPP)1996 • Health Information Act (HIA) 2015 	<p>The amended ATIPP Act for the Northwest Territories came into effect on July 30, 2021 and municipalities are now covered under it.</p> <p>The Act will now provide improved public accountability through access to government information, as well as more safeguards for how personal information is collected, used, and disclosed by public bodies.</p>

Jurisdiction	Legislation Enacted	Amended and For What Purpose
		Permits the collection and disclosure of information for the delivery of common or integrated programs and services.
NU	<ul style="list-style-type: none"> Consolidation of Access to Information and Protection of Privacy Act 1994 	No amendments.
ON	<p><u>PUBLIC SECTOR</u></p> <ul style="list-style-type: none"> Freedom of Information and Protection of Privacy Act (FIPPA) 1990 Municipal FIPPA 1990 Personal Health Information Protection Act (PHIPA) 2004 <p><u>PRIVATE SECTOR</u></p> <ul style="list-style-type: none"> Bill 64 to enact private sector privacy legislation 2021 	<p>Ontario’s provincial access and privacy law was amended in 2019 and 2020 to enable data integration units to indirectly collect and link personal information – within and across ministries, and even with designated external entities – for the purpose of analyzing, managing, planning and evaluating government programs and services. The amendments to <i>PHIPA</i> establish a comprehensive privacy and accountability framework for the provincial electronic health record, allocating shared responsibilities among multiple custodians using the record.</p> <p>Not yet enacted.</p>
PEI	<ul style="list-style-type: none"> Freedom of Information and Protection of Privacy Act 1988 Health Information Act 	No amendments.
QC	<ul style="list-style-type: none"> Act respecting Access to documents held by public bodies and the Protection of Personal Information 2006 Act to amend the Act respecting Health Services and Social Services, the Health 	<p>In June 2020, the government of Quebec introduced Bill 64, <i>An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information</i>.</p> <p>(Not yet enacted.)</p>

Jurisdiction	Legislation Enacted	Amended and For What Purpose
	<p>Insurance Act and the act respecting the Regie de l'assurance maladie du Quebec</p> <ul style="list-style-type: none"> Act to amend the Act respecting the governance and management of the information resources of public bodies and government enterprises and other legislative provisions <p>PRIVATE SECTOR</p> <ul style="list-style-type: none"> Act Respecting the Protection of Personal Information in the Private Sector 2021 	(Received assent, not yet implemented.)
SK	<ul style="list-style-type: none"> The Freedom of Information and Protection of Privacy Act (FOIP) 1990 Local Authority Freedom of Information and Protection of Privacy Act- municipal public sector 1991 The Health Information Protection Act (HIPA) 2003 	
YT	<ul style="list-style-type: none"> Access to Information and Protection of Privacy Act (ATIPP) 2018 Health Information Privacy and Management Act 2013 	<p>The Yukon Legislative Assembly has passed the new Access to Information and Protection of Privacy Act, Bill 24, which will come into force on April 1, 2021 to:</p> <ul style="list-style-type: none"> provide integrated services in collaboration with partner agencies; provide a government-wide personal identity service; and, carry out data-linking activities.