

ADDRESSING LEGISLATIVE, POLICY AND DATA SHARING BARRIERS TO INTEGRATED AND SEAMLESS SERVICE DELIVERY ACROSS LEVELS OF GOVERNMENT

ISSUE

At the February 28, 2019 meeting of the Public Sector Service Delivery Council (PSSDC), an action item was assigned to the co-chairs of PSSDC to develop a problem statement/case for addressing legislative and data sharing barriers impeding the advancement of some Joint Councils and PSSDC priorities. Many government services provided to Canadians would benefit from more integrated inter-jurisdictional service delivery to improve the client experience. Achieving seamless service has proven to be challenging in the current federal-provincial-territorial-municipal context.

At times, legislation intended to protect client privacy or define the nature of inter-jurisdictional collaboration and/or the interpretation of this legislation in associated policy instruments, may have inadvertently created barriers to delivering more seamless services. Examples of barriers include limitations on sharing client information that would support a “tell us once” approach, limitations on sharing data to support data analytics, and the degree to which one level of government can provide services on behalf of another level of government. These challenges are affecting several of the priorities of Joint Councils/PSSDC, including Digital Identity, Death Notification, Service to Business and Data Driven Intelligence (DDI).

Advancing technology presents new ways of collaborating that may require changes to legislation or administrative policy to reap the anticipated benefits, while also respecting citizens’ privacy and upholding public trust in government. Complexities in addressing legislative, policy and data sharing barriers cannot be resolved quickly, and therefore, a systematic approach for addressing the challenges is required.

CONTEXT

The issue is timely. Canadian and many international governments, in addition to several Joint Councils working groups, are exploring the legislative, policy and data sharing landscape affecting service delivery. Examples are provided in Annex A and include:

- Federally, the Treasury Board of Canada Secretariat (TBS) is conducting a horizontal review of information sharing and privacy in Government of Canada (GoC) service delivery
- Provincially/territorially, legislative efforts around sharing of information are being implemented in Ontario, Quebec and Saskatchewan
- Inter-jurisdictionally, the
 - Joint Councils Digital Identity priority MyAlberta Digital ID (MADI) pilot has considered concerns about the collecting, disclosing and protecting of personal information as part of the fundamental planning for the project,
 - PSSDC DDI Working Group has been tasked through the FPT DMs’ Table on Service Delivery Collaboration to develop an action plan addressing legislation, privacy and data sharing issues
 - Joint Councils General Data Protection Regulation (GDPR) Working Group, under the Privacy Sub-Committee, is analyzing the implications of the new European Union GDPR legislation
- Internationally, legislative efforts around data sharing between public organizations have taken place or are underway in Australia, Belgium, and the United Kingdom

These examples underline the need for a dialogue to develop a clear and comprehensive understanding of the scope of the issue, and identify which legislative, policy and data sharing barriers are real versus perceived. They also demonstrate that new models and approaches are being developed which could provide prototypes for future solutions in other jurisdictions

PROPOSED APPROACH

It is proposed that recommendations be developed to address legislative, policy and data sharing barriers affecting the advancement of the following key Joint Councils/PSSDC priorities: Digital Identity, Death Notification, Service to Business and DDI. The tasks to be included in a work plan could encompass:

- Developing an understanding of what are the specific legislative, policy and data sharing barriers affecting each of the four priorities, through identification of specific use cases in order to support analysis, recognizing the legal and policy analysis will be specific to what is being shared, with whom and for what purpose, and that generalization of barriers will be difficult
- Confirming which barriers are real versus perceived
- Assessing which barriers should be addressed first, considering factors such as overall impact in advancing one or more of the priorities and possible “quick wins”
- Completing an environmental scan of other federal-provincial/territorial-municipal committees that may be addressing similar barriers
- Completing an environmental scan to determine what other jurisdictions or countries have done to address the top barriers
- Developing recommendations to address the top barriers including the proposed model(s), use case(s) and inter-jurisdictional pilot(s) to test the recommendations

The emphasis of this work will be on determining what are the real versus perceived barriers, recognizing that Joint Councils are more likely to be able to influence administrative policy to facilitate more seamless service delivery rather than legislation, which is the purview of each jurisdiction’s parliament and difficult to change in the short term. While there are also technical complexities around inter-jurisdictional sharing of data, this is considered beyond the scope of this work.

There are several options for undertaking this work:

- A. Assigning this work to the Privacy Sub-Committee.** A key legislative and data-sharing barrier revolves around privacy. As lead, the Privacy Sub-Committee would reach out to the four priority working groups, the GDPR Working Group and the Research Committee to get the necessary input and to develop project deliverables.
- B. Assigning this work to the Data Driven Intelligence Working Group:** At the meeting of the FPT DMs’ Table on Service Delivery Collaboration on June 20, 2019, the DDI Working Group was tasked to develop an action plan addressing issues including legislation, privacy and data sharing. Should the DDI Working Group be the preferred lead, a federal co-chair could be sought to provide a federal perspective and support the provincial and municipal DDI co-chairs in the work. The DDI Working Group would reach out to the four priority working groups, the Research Committee, the Privacy Sub-committee and the GDPR Working Group to get the necessary input and develop project deliverables. Addressing a broad range of data-sharing barriers, in addition to privacy, would fit with the DDI Working Group’s mandate.

- C. **Establishing an adhoc time-limited Joint Councils Task Team:** This team would be co-chaired by a federal and a provincial/territorial/municipal (PTM) representative, with interested jurisdictions as members responsible for implementing the proposed outlined above.

PROPOSED TIMELINE

- October 2019 – September 2020

RECOMMENDATION

- Assign the Data Driven Intelligence Working Group to develop the proposed approach/workplan (Option B)
- Proceed to undertake the work as outlined in the approach above, with \$60K earmarked to support fleshing out the problem definition and use case exploration
- Seek a federal co-chair for DDI to provide a federal perspective and support the provincial and municipal DDI co-chairs in the work

NEXT STEPS

- Confirm approach and leads for this work
- Develop terms of reference and detailed work plan

DISCUSSION QUESTIONS

1. Do Joint Councils agree on the following:
 - The framing of the issue (what problem are we trying to solve)?
 - The proposed approach/workplan?
 - That the DDI WG is the appropriate governance model to move this work forward?

Examples of Canadian and international governments that are considering or have implemented legislative changes having implications for more seamless integrated service in a digital age.

Federal

Treasury Board Secretariat of Canada is engaged in a horizontal review of information sharing and privacy in Government of Canada (GoC) Service Delivery. This review complements the federal Privacy Act review as well as efforts to advance the GC Data Strategy and related commitments to promote greater strategic use of data while safeguarding privacy. The exercise involves identifying and addressing key policy and legal barriers that get in the way of the GoC's vision for seamless, digital services through three streams of work:

- The need and options for a single file number
- Simplifying the information sharing process
- Separate perceived from real legislative barriers

Canada's Privacy Act (s. 8.2 (f)) requires federal institutions to establish an agreement or arrangement to disclose personal information under its control to other levels of government or jurisdictions. The degree of inter-jurisdictional collaboration is also influenced by other legislation and policies including Canada's Federal Income Tax Act and departmental acts such as the recently updated Department of Employment and Social Development Act (DESDA).

The **Service Canada and Canada Revenue Agency (CRA) Direct Deposit and Address Information Sharing initiative** has leveraged the Social Insurance Number so that with consent, Canadians' banking information is updated for certain CRA/ESDC benefits and credit programs and income tax returns and shared between these two organizations.

Provincial/Territorial

In June 2019, **Ontario** passed a new bill (Simpler, Faster, Better Services Act) which, in part, amended the Freedom of Information and Protection of Privacy Act (FIPPA) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). This initiative was meant to enable public sector bodies to share personal information with law enforcement without consent. A more extensive set of amendments to FIPPA is being developed.

In April 2019, **Quebec** introduced legislation (An Act to facilitate the public administration's digital transformation) which includes rules applicable to sharing of personal information, essentially enabling a "tell us once" approach to accessing government services. In its 2019-2023 strategic plan, **Quebec's** privacy commission expressed a need for legislative amendments to positively influence public trust in the government and to facilitate collaboration with other jurisdictions.

Saskatchewan recently implemented changes to its legislation to create a more enabling environment for data analytics.

Inter-jurisdictional

The **MyAlberta Digital ID pilot** is a collaborative effort between Alberta, ESDC and TBS that allows Albertans with a verified MyAlberta Digital ID to have real time access to their My Service Canada Account using the Pan Canadian Trust Framework (PCTF). Concerns about collecting, disclosing and protecting personal information have been part of fundamental planning for this project.

At the meeting of the FPT DMs' Table on Service Delivery Collaboration on June 20, 2019, the **Data Driven Intelligence** priority Champion (Manitoba) called on jurisdictions to create an enabling environment for advancing the value of analytics, including the development of a data-sharing framework, and building data literacy for analysis and decision-making. The DDI Working Group was tasked to develop an action plan addressing issues including legislation, privacy and data sharing.

The Joint Councils **General Data Protection Regulation (GDPR)** Working Group, under the Privacy Sub-Committee is analyzing the European Union GDPR that came into effect in May 2018 and harmonizes data protection across EU member states into one single law to provide more control of personal data to EU citizens. Under GDPR, transfer of data to third countries is regulated by an 'adequacy decision' that requires a third country to have an adequate level of protection for privacy as exists in the EU through the GDPR.

The **Canadian Council of Motor Transport Administrators (CCMTA)** is undertaking work to modernize the interprovincial record exchange system (which facilitates the sharing of driver and vehicle data nationally) with a view to supporting digital ID at a national level. The CCMTA coordinates all matters dealing with the administration, regulation and control of motor vehicle transportation and highway safety. Membership includes representation from provincial and territorial governments as well as the federal government. Since every PT utilizes the IRE to share data, there may be an opportunity to influence the requirements of the IRE modernization project to facilitate the sharing of data nationally, especially around a digital ID.

The **CIO Strategy Council** has drafted a third-party access to data and privacy standard which is currently under public review with the **Standards Council of Canada**.

<https://ciostrategyCouncil.com/standards/draft-standards/>

International

Australia recently introduced the Data Sharing and Release Bill to share data across all layers of government for any purposes including administration, service delivery and research, provided the appropriate level of risk management is in place. Subject to certain conditions, the bill allows the Australian Government to share and release Australian Government data with states and territories and with non-government sectors.

Belgium's Crossroads Bank for Social Security coordinates implementation of e-government projects within the social sector through the use of a National Register Number. **Estonia** has a single government database of personal information accessible to all government entities. The **United Kingdom** attempted to implement a National Identity Registry; however, it was discontinued in response to an outcry from privacy experts.

The **Netherlands General Digital Infrastructure (GDI)** unites various service delivery ministries, provinces, public utility companies and many executive organizations of the Netherlands. It facilitates service delivery to citizens and businesses through secure, cost effective, standardized and structured electronic data sharing. It uses 13 data registries/bases with 'once only' data provision and multiple usage capacities.

DRAFT