Discussion Paper: Privacy and Justice Sector Research and Evaluation

By David Loukidelis, QC
for

Access to Justice Metrics Colloquium
February 27, 2020, Victoria BC

david@loukidelis.ca
1 587 985-2818

DISCUSSION PAPER:
PRIVACY AND JUSTICE SECTOR RESEARCH AND EVALUATION[1]

David Loukidelis QC

Access to Justice Metrics Colloquium
February 27, 2020 Victoria BC

INTRODUCTION

This paper is intended to help inform justice sector participants about British Columbia's privacy rules as they relate to justice system research, evaluation and planning activities. It is intended to support general discussion of those laws at the colloquium. It also illustrates how those laws protect individuals' privacy while enabling beneficial research into important public policy questions.

This paper takes it as given that there is a consensus among many participants in British Columbia's civil justice system that access to justice can be enhanced through research, evaluation and analysis of data.[2] Those activities of course depend on creation of meaningful and appropriate performance metrics and therefore timely availability of relevant, accurate data. A key goal of the Action Committee Metrics Working Group and other bodies, therefore, is to make more and better data available to researchers, to enhance the capacity of our civil justice system to measure program performance and evaluate user outcomes.[3]

The public interest in facilitating research has long been reflected in British Columbia's legislated privacy framework, which explicitly permits researchers to gain access to fully identifiable personal information for research purposes. This said, researchers very rarely, almost never, seek fully identifiable information. They are interested in populations and systems, not individuals, i.e., their quest for knowledge is not about individuals in any immediate sense. It is important to mention this up front, as this observation applies to the justice sector with the same force as it does to other kinds of research. This must be kept in

[1] The views expressed here are solely the author's, as are any errors or omissions.
[2] The term "research" is used below for convenience, to encompass research in its broadly understood meaning as well as analytical and evaluative efforts that strictly speaking might not be research yet aim to yield information or knowledge about a particular matter.
[3] This requires, among other things, harmonizing of data definitions and identification of data sets that can foster cross-jurisdictional research through the appropriate sharing of data for research and evaluation. These issues are not addressed here.

mind whenever data sharing is being discussed, since the corollary is that de-identified information is the currency of research, not identifiable information.

While a great deal of the personal information needed for justice system research and analysis is collected or created by public bodies, some information rests in the private sector. Both sectors are covered by privacy laws that regulate the collection, use and disclosure of personal information. At the point of collection information needed for research will often be about identifiable individuals, i.e., "personal information".[4] This information is rarely, if ever, used in identifiable form, however. It is almost invariably the case that, after collection, personal information is de-identified before researchers are permitted to use it.[5]

One challenge for researchers is that data holdings are often fragmented, with a range of public and private sector sources of data that they need for research. In recent years many have identified the need to fashion a streamlined data sharing governance structure and, ideally, a centralized research infrastructure. This has been prompted in part by the experience of health researchers in British Columbia, who have been confronted by a diffuse and largely uncoordinated approach to access to health data for research. Many health research requests involve data held by multiple public bodies, each of which approves access and often does so applying differing approval criteria and processes. Laudable, meaningful improvements have undoubtedly been made in recent years, but this experience suggests that, in the justice sector, care should be taken to, if possible, take a one-window approach to data access approvals. The same point applies to the technical aspects of data holdings. Multiple data stores almost certainly impose unnecessary capital and operating costs that a scaled-up single repository can avoid. Further, a system in which there are multiple data holdings is likely to increase security data risks. Examples include risks flowing from weak data access governance, thanks to varying criteria and processes, and the risk of data loss from multiple holdings.[6]

Steps have been taken in recent years to address these challenges. This is well illustrated by the provincial government's Data Innovation Program. Under the authority of British Columbia's public sector privacy law, the *Freedom of Information and Protection of Privacy Act* (FIPPA), and the provincial *Statistics Act*, the Data Innovation Program integrates data from ministries in a secure platform. The Data Innovation Program is hosted by the Office of the Chief Information

[4] As noted below, the relevant British Columbia statutes define "personal information" as "information about an identifiable individual". (For convenience, this paper sometimes uses the term "data" as a short-hand form of "personal information".)

[5] De-identified methods vary, but great deal of expertise exists in the British Columbia public sector in de-identification of personal information.

[6] Even if lost data cannot realistically be re-identified, the public perception consequences will be negative and difficult if not impossible to counter.

Officer and operates under the statutory authority of the Director of Statistics and the minister responsible for the *Statistics Ac*t.[7]

Data contributed to the Data Innovation Program are held at Population Data BC, a contracted service provider. Population Data BC, which is located at the University of British Columbia, has operated for some 20 years. Its role is to house a broad range of health and other data for use by researchers. It is a highly respected organization.

It keeps all data in secure servers located in a physically secure, access-controlled, location at the University of British Columbia. Approved researchers who use Population Data BC's holdings do not remove data from its secure research environment. They are given access to data extracts necessary for each individual research project. They analyse the data within Population Data BC's secure environment, with the results of their analyses being made available to them.

The data that ministries contribute to the Data Innovation Program are linked at the individual level but are de-identified. Data contributed to the Data Innovation Program are not kept or linked with other data held by Population Data BC. Researchers using use the data for population-level research. They do not use it for individual-level activities.[8]

Access to data is permitted only for researchers and projects that have been approved by the Data Innovation Program. The Data Innovation Program processes all research outputs—including reports, articles, briefing papers, data tables and other similar products—using both technological statistical disclosure controls and manual review by a statistical disclosure expert to ensure the outputs do not contain any personal information.

Before outlining how British Columbia's privacy laws work in this context, the next part of this paper supports colloquium discussion through examples of the kinds of research in which justice sector participants might engage.

[7] The Data Innovation Program has a chief privacy and security officer and a privacy and security framework. A privacy impact assessment was completed as the Data Innovation Program was being developed.

[8] This is reinforced by the *Freedom of Information and Protection of Privacy Act* and by section 6 (1) of the *Statistics Act*, which prohibits use of information collected under that Act "to the prejudice of any person."

JUSTICE SECTOR RESEARCH PARTICIPANTS

A useful overview of how British Columbia regulates privacy requires a shared understanding of which possible civil justice system participants can be identified are in the public sector and private sectors. A shared view of some purposes for which various participants might share data also aids discussion. The following overview is intended to achieve these goals.

Public sector participants

Public sector participants in the civil justice system, and some of the purposes for which they might share personal information, include these:[9]

- All three levels of court, *i.e.*, the Provincial Court, the Supreme Court and the Court of Appeal. A court might share data to assess accessibility to the court for Indigenous people or newcomers to Canada. The courts might share personal information with others in order to assess public confidence in the courts and the civil justice system overall.[10]
- Administrative tribunals such as the Civil Resolution Tribunal, Human Rights Tribunal, Residential Tenancy Branch and Employment Standards Tribunal. Tribunals might share personal information for similar purposes.
- Ministry of Attorney General lawyers involved in child protection matters and perhaps other civil litigation matters involving individuals as parties. Other Ministry employees, such as family justice counsellors, who interact with clients. As the ministry responsible for the administration of justice, the Ministry might share data for a very wide range of purposes related to program efficiency, including in court administration, and for purposes such as those already suggested.
- Legal Services Society, whether through its own employees or outside counsel retained in civil matters. It may collect personal information from individuals when surveying individuals' experiences with access to justice, as it did in 2013 and 2018.[11]
- Law Foundation of British Columbia, which, through its funding of research projects, may hold personal information that funded researchers have made available to the Law Foundation.[12]

---

[9] For clarity, neither these nor the examples of private sector participants are intended to be comprehensive, as that is not necessary for present purposes. The same holds for the examples of the kinds of data sharing in which various participants, including the courts, might or might not engage. The examples are the author's and are offered solely to facilitate understanding of how privacy laws work.

[10] None of British Columbia's three courts is subject to a privacy statute. It is open to each court to decide if it wishes to adopt a privacy policy and governance framework, generally or in relation to research matters.

[11] The Legal Services Society is included as a public sector body because it is designated a "public body" and is thus covered by British Columbia's public sector privacy law, the *Freedom of Information and Protection of Privacy Act*.

[12] The Law Foundation is also designated as a "public body" under FIPPA.

Private sector participants

These are some obvious examples of private sector actors in our civil justice system:

- Lawyers in private practice. They may share data to participate in an evaluation conducted by the Ministry of Attorney General or by the Legal Services Society.
- Mediators and other ADR practitioners. They may wish to share data to participate in an evaluation conducted by the Ministry or by the Legal Services Society.
- Public legal information providers and Access Pro Bono.

Keeping these examples in mind, the next section offers an overview of British Columbia's privacy legislation.

KEY FEATURES OF BRITISH COLUMBIA'S PRIVACY LAWS

Both sectors are subject to statutory privacy regimes that govern the collection, use and disclosure of personal information. The most salient aspects of British Columbia's privacy laws are summarized below, for discussion purposes.

Public sector privacy[13]

The *Freedom of Information and Protection of Privacy Act* (FIPPA) is British Columbia's privacy law of general application in the broad public sector, regulating public bodies' collection, use and disclosure of personal information. It applies to thousands of public bodies at all levels, but not the courts.

What is "personal information"?

The term "personal information" means "recorded information about an identifiable individual".[14] As the term "identifiable" suggests, information may qualify as "personal information" even if the individual it is about is not explicitly named. The Information and Privacy Commissioner, an officer of the Legislature, has made it clear that information will qualify as personal information if an individual can be identified using that information alone,

[13] The federal public sector privacy law, the *Privacy Act*, is not discussed here because it is unlikely to apply in the context of research and evaluation relating to British Columbia's civil justice system. It applies only to federal government departments, Crown corporations and their designated subsidiaries.

[14] The definition excludes "contact information". This is defined as "information to enable an individual at a place of business to be contacted", including the individual's "name, position name or title, business telephone number, business address, business email or business fax number".

or in combination with other available information, with the application of reasonably available techniques.

To which bodies does FIPPA apply?

FIPPA applies to a wide range of public bodies, including provincial government ministries, local governments, universities, school boards, health care bodies (including health authorities and hospitals), and prescribed agencies and bodies (including tribunals such as the Civil Resolution Tribunal and the Human Rights Tribunal). Each provincial government ministry is a public body, meaning that the Ministry of Attorney General and the Ministry of Solicitor General and Public Safety are separate public bodies. This means that the Court Services Branch and Criminal Justice Branch are subject to FIPPA. By contrast, as noted earlier, none of the three courts in the province is a "public body", meaning that FIPPA does not regulate their collection, use or disclosure of personal information.

Limits on FIPPA's application

FIPPA applies to all records in the custody or under the control of a public body, "including court administration records," but expressly does not apply to "a court record, a record of a judge of the Court of Appeal, Supreme Court or Provincial Court, a record of a master of the Supreme Court, a record of a justice of the peace, a judicial administration record or a record relating to support services provided to the judges of those courts".[15] Nor does it apply to "a personal note, communication or draft decision of a person who is acting in a judicial or quasi-judicial capacity"[16] or "a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed".[17]

Collection of personal information

Unless Part 3 of FIPPA authorizes it to do so, a public body cannot collect, use or disclose personal information. The following discussion outlines the rules for collection, use and disclosure, with special attention to the implications for research, analysis and evaluation.

The heads of authority for personal information collection are reasonably generous. Most relevant for present purposes, a public body may collect personal information if:

[15] Section 3(1)(a).
[16] Section 3(1)(b).
[17] Section 3(1)(h).

- The collection is expressly authorized under an Act,
- The information is collected for the purposes of "law enforcement",[18]
- The information relates directly to and is necessary for a program or activity of the public body,
- The information is necessary for the purposes of planning or evaluating a program or activity of a public body.

Individual consent can sometimes play a role. FIPPA authorizes collection of personal with consent where the collection is for a prescribed purpose, the individual has consented in the prescribed manner and a reasonable person would consider that collection appropriate in the circumstances.

A public body must collect personal information directly from the individual the information is about unless indirect collection is authorized by that individual, another enactment, or the Information and Privacy Commissioner. Personal information may also be collected indirectly if it may be disclosed to the public body that uses it under other provisions of Part 3. A public body may also collect personal information indirectly if the collection is necessary for delivering or evaluating a common or integrated program or activity (a term that is defined in FIPPA).

Public bodies are also required to give individuals notice of the purpose for collecting their personal information, the legal authority for collecting it and public body contact information (so that an individual can ask questions about the collection). The notice requirement is dispensed with where indirect collection is authorized (notice is also not required in certain other cases).

Use of personal information

Personal information in the custody or control of a public body may only be used for the purpose for which it was obtained or compiled, or for a use that is consistent with the purpose for which it was collected.[19] In addition, personal information may be used if the individual information is about has identified it and consented, in the prescribed manner, to the use. Last,

[18] The term "law enforcement" is defined as "policing, including criminal intelligence operations", "investigations that leader could lead to a penalty or sanction being imposed", or "proceedings that lead or could lead to a penalty or sanction being imposed". It is recognized that this collection authority is hardly at the forefront for civil justice system evaluation; it is mentioned for completeness, since there may be a situation in which linkages are sought between civil justice and criminal justice data, or policing, data for evaluation purposes.

[19] A new use of personal information will be consistent with the purpose for which it was obtained or compiled if the new use as a reasonable and direct connection to the purpose for collection and the new use is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.

a public body may use personal information for a purpose for which it may be disclosed to that public body under Part 3.

Disclosure of personal information

As with collection and use, a public body's ability to disclose personal information depends on specific statutory authority under Part 3. The situation is somewhat complicated by the distinction between disclosure of personal information outside Canada and disclosure inside Canada. Only the latter type of disclosure is dealt with here, since it seems highly unlikely that justice system evaluation will involve disclosure of personal information—as opposed to disclosure of research or evaluation outcomes—outside Canada.

Among other things, FIPPA authorizes a public body to disclose personal information:

- If the individual the information is about has identified the information and consented in the prescribed manner,
- In accordance with a British Columbia or federal enactment that authorizes or requires the disclosure,
- Where the information is made available to the public in British Columbia under another enactment that authorizes or requires information to be made public,
- To a public body employee and the information is necessary for performance of his or her duties,
- To an employee of a public body or an "agency",[20] or a minister, if that information is necessary for the delivery of a "common or integrated program or activity" and the performance of the recipient's duties respecting that program or activity,
- To an employee of a public body, or to a minister, if the information is necessary for the purposes of planning or evaluating a program or activity of a public body,
- If the disclosure is for a research purpose, as noted below.

Regarding research, FIPPA authorizes public bodies to disclose personal information in their custody or control for a research purpose, including statistical research, subject to certain conditions. It is important to underscore that public bodies are authorized to disclose fully identifiable information about individuals so long as the first FIIPA condition is met, *i.e.*, it must be the case that the research purpose cannot reasonably be accomplished unless the

[20] The term agency is defined to include a federal government institution, a private sector organization covered by BC's private sector privacy law, a private sector organization covered by the federal private sector privacy law, a comparable body covered by provincial legislation having the same effect as FIPPA. As discussed below, inclusion of private sector organizations expands the scope of possible privacy governance across the sectors.

information is provided in individually identifiable form (or the Information and Privacy Commissioner has approved the research purpose).

Several other conditions apply to research disclosures. The first is that the information must be disclosed on the condition that not it be used to contact a person to participate in the research. Second, it must be the case that any data linking is not harmful to the individuals the information is about and the benefits to be derived from the linking must be clearly in the public interest. Last, the recipient must sign an agreement to comply with conditions the public body has approved relating to security and confidentiality, the removal or destruction of individual identifiers at the earliest reasonable time, and prohibition of any subsequent use or disclosure of the information in an individually identifiable form (unless the public body expressly authorizes it).

The disclosure and use of personal information for research purposes is addressed in more detail at the end of this paper, largely to illustrate how a coordinated, delegated approach to research infrastructure would be desirable in the interests of advancing effective justice sector research.

Although FIPPA's rules on use of personal information for research are at the heart of this paper, it is useful to outline how it also enables use of personal information for other beneficial purposes. It is first necessary to outline British Columbia's private sector privacy rules, including to illustrate how they align, on the research issue, with FIPPA.

Private sector privacy[21]

The *Personal Information Protection Act* (PIPA) governs the collection, use and disclosure of personal information by private sector organizations. Compliance is overseen by the OIPC.

What is "personal information"?

At its core PIPA's definition of "personal information" is the same as FIPPA's, "information about an identifiable individual", the only real difference being that PIPA does not, on its face, apply only to "recorded" personal information.[22]

---

[21] The federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), is not likely to be relevant. It does not apply to organizations in British Columbia that are subject to PIPA. It applies to federal works, undertakings and businesses in British Columbia, however.

[22] For present purposes—for most purposes—this distinction will be irrelevant. Also, see the earlier comment about identifiability, in the discussion of "personal information" under FIPPA.

To whom does PIPA apply?

The legislation applies to private sector organizations, including a person, an unincorporated association, a trade union, a trust or a not-for-profit organization. The term "organization" does not include an individual acting any personal or domestic capacity or acting as an employee, a public body, or any of the three courts in British Columbia.[23] PIPA's definition of "organization" extends to law firms, lawyers practising as sole practitioners, mediators and other private-sector actors offering services to clients.

Limits on PIPA's application

PIPA does not apply to personal information in a court document, a document of a judge or a document relating to support services provided to a judge.[24] It also does not apply to a court administration record. Similarly, PIPA does not apply to personal information if FIPPA applies to it, which is obviously an attempt to dovetail the two statutes.[25]

Consent to collection, use or disclosure of personal information

In contrast to FIPPA, the default under PIPA is that an organization may only collect, use or disclose personal information with the consent of the individual, unless PIPA authorizes it without consent (or deems consent to have been given). The statute contains several requirements related to consent, such as a requirement for notice of the purpose for collection, a prohibition against giving false or misleading information in order to obtain consent, and the ability of individuals to withdraw consent. PIPA also sets out rules relating to deemed consent and imposes constraints on when consent may be required.[26] it is not necessary to discuss any of these rules for present purposes, although they should be kept in mind as matters unfold.

---

[23] It also excludes the Nisga'a Government and a private trust the beneficiaries of which are friends or members of the family of the settlor.

[24] It also does not apply to a record of a master or justice of the peace.

[25] Nor does PIPA apply to personal information if the federal private sector privacy law, PIPEDA, applies to that personal information.

[26] In the latter case, PIPA provides that an organization must not, as a condition of supplying a product or service, require an individual to consent to collection, use or disclosure of personal information beyond what is necessary to provide the product or service. Similarly, an organization may collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that fulfil the purposes of which the organization gives notice to the individual at or before the time of collection.

Exceptions to consent

PIPA permits non-consensual collection, use and disclosure of personal information for a range of purposes. Most relevant for present purposes, an organization may collect, use or disclose personal information without consent:

- Where the personal information is available to the public from a prescribed source,
- If the collection is required or authorized by law,
- Where the disclosure is for a research purpose (subject to conditions that are substantially the same as those described above for research disclosures under FIPPA).

Other requirements

Like FIPPA, PIPA imposes other rules, including those relating to protection of personal information from privacy breaches, an individual's right of access to her or his own personal information, the right to request correction of personal information, and so on.

As is the case under FIPPA, the OIPC has, in its guidance for the private sector, stated that it expects organizations to demonstrate accountability for compliance through privacy management frameworks that include policies and procedures for managing compliance, responding to privacy breaches and more.[27]

JUSTICE SECTOR RESEARCH & PRIVACY

From a purely legal perspective the authority under FIPPA and PIPA is the most straightforward tool for research in the justice sector. This is because the statutory authority to collect, use and disclose personal information for research purposes is essentially the same under both laws. The applicable statutory conditions for disclosure are also essentially the same. There are, however, practical challenges in using that authority in a justice sector that spans both public and private sectors and has many participants. The challenges relate to, among other things, resources, expertise and institutional capacity.

[27] The OIPC also promotes the use of privacy impact assessments and is likely to expect information sharing agreements as part of any common or integrated program or activity arrangement.

Specifically, application of the statutory authority, and compliance with the accompanying rules, raises these challenges (and likely others):

- Whether personal information may be disclosed for a research purpose must be assessed on a case-by-case basis. This inevitably involves project-specific research applications. Unless all relevant justice sector participants delegate their functions in this area to a single decision-maker, they will each have to consider each research application.
- The costs involved in having each participant create and operate its own research disclosure program are likely to be significant. The delays involved for researchers in having to obtain multiple approvals from various data holders, each of whom may well apply differing standards and procedures, are likely to be significant. For example, in both sectors, each disclosing party must satisfy itself, in each case, that the disclosure is truly for a "research" purpose. This exercise requires some expertise in research.
- Further, both statutes stipulate that information in individually identifiable form may only be disclosed if the research purpose otherwise cannot otherwise reasonably be accomplished. In cases where a research purpose *can* "reasonably be accomplished" without "information in individually identifiable form", it is necessary to de-identify the personal information. This must be done by the party disclosing the information, and it must be done through case-by-case analysis by staff who are knowledgeable in research techniques and associated technical matters.
- If de-identification is necessary, the disclosing party must de-identify the data applying technical expertise guided by that party's established de-identification policies and techniques (which may vary across the sector).[28]
- If the research involves data linking, the disclosing party must be satisfied, based on the research application, that the linking is not harmful to the individuals involved and that the benefits to be derived from the linking are clearly in the public interest. This again raises the challenges of cost and expertise.
- In all cases, the disclosing party must approve conditions related to security and confidentiality, removal or destruction of individual identifiers at the earliest reasonable time, and prohibition on any subsequent use or disclosure of the information. These conditions must be secured by a research agreement between the disclosing party and the researcher. The same challenges arise.
- These processes obviously require dedicated expert resources, either in-house or using service providers with the necessary expertise. The compliance costs for each participating public body and organization can quickly mount up. The systemic resource implications are undoubtedly significant in a world where each participating public body and organization

[28] As machine learning techniques improve, achieving de-identification that is secure against re-identification attempts is increasingly a challenge.

replicates these functions. The systemic costs could be mitigated to a degree by having all sector participants adopt uniform standards, policies and procedures, but the implementation costs would continue unless these functions are delegated to a central decision-maker.

These considerations favour a coordinated, cross-sector approach to the disclosure and use of data for justice sector research. Delegation to a trusted, expert institution of the authority to give access to data for justice sector research, and the responsibility for protecting the data, could advance the cause of beneficial public policy research in the sector while ensuring robust privacy protection.

CONCLUSION

As this paper underscores, British Columbia's privacy laws undoubtedly support the collection, use and disclosure of personal information for research in the public interest while meaningfully protecting individual privacy. It is broadly understood that many British Columbians face hurdles in gaining access to justice. Surely all can agree that the justice sector ought to identify, understand and address the barriers they face through research into the causes and possible solutions. The work needed to do this requires a cooperative, respectful approach to the sharing of data and its use for beneficial research in this area.

***