Discussion Paper

EXPLORATION OF THE IMPACT OF CANADA'S INFORMATION MANAGEMENT REGIME ON FIRST NATIONS DATA SOVEREIGNTY

FNIGC | CGIPN
First Nations Information Governance Centre
Le Centre de gouvernance de l'information des Premières Nations

August 2022

FNIGC | CGIPN
First Nations Information Governance Centre
Le Centre de gouvernance de l'information des Premières Nations

First Nations Information Governance Centre
341 Island Road, Unit D
Akwesasne, ON K6H 5R7

Tel: 613-733-1916
Toll Free: 866-997-6248

fnigc.ca

ISBN: 978-1-988433-16-5

Our Work

FNIGC is committed to providing quality information that contributes to improving the health and well-being of First Nations people in Canada.

In collaboration with our regional partners, FNIGC conducts unique data-gathering initiatives that enable our partners to support First Nations governments to build culturally relevant portraits of their communities.

FNIGC supports First Nations communities by contributing directly to building data and statistical capacities at national, regional, and community levels, including the provision of credible and relevant information on First Nations. In addition to conducting a number of surveys, FNIGC is responsible for a wide range of other work. We oversee data collection on First Nations reserves and in northern communities, conduct research, engage in knowledge translation and dissemination activities, offer education and training, and promote the advancement of the First Nations principles of OCAP®.

Critically, FNIGC and our regional partners follow established protocols, policies, and procedures that are guided by a holistic cultural framework.

Contents

Executive Summary

The First Nations Information Governance Centre (FNIGC) is an incorporated, non-profit organization committed to producing evidence-based research and information that will contribute to First Nations in Canada achieving data sovereignty in alignment with their world views. The FNIGC is strictly technical and apolitical and is not a rights-holding organization. The FNIGC does not speak directly for First Nations. Mandated by the Assembly of First Nations' Chiefs-in-Assembly (AFN *Resolution #48*, December 2009), the mission of FNIGC is to strengthen First Nations data sovereignty and foster the development of information governance and management at the community level. We adhere to free, prior and informed consent, respect Nation-to-Nation relationships, and recognize the distinct customs of First Nations, to achieve transformative change. Our work includes research and analysis of the technical elements of First Nations data sovereignty, like information management.

This discussion paper explores the conflicts between the current Canadian information management regime and First Nations data sovereignty. At the time of writing, Canada is reviewing the *Privacy Act* with a view to amendments and is conducting a five-year review of the *Access to Information Act*. In response, the federal government undertook a review of the *Privacy Act*. (Minister of Justice, 2017). As part of the review, the Department of Justice (DOJ) issued a series of discussion papers on the *Privacy Act* inviting public comment (DOJ, 2019; DOJ, 2020). Each of the first four 2019 discussion papers raise issues of relevance to First Nations data sovereignty. In addition, there is a fifth paper specifically on *Modernizing the Privacy Act's relationship with Canada's* [sic] *Indigenous peoples* (DOJ, 2019e). Based on a first round of dialogue, additional considerations for reflection were presented by DOJ in 2020 (DOJ, 2020). This includes recognizing the objective of advancing reconciliation with First Nations through amendments to the *Privacy Act*.

FNIGC acknowledges the challenges with the *Privacy Act* identified by the Standing Committee and DOJ. To respect First Nations data sovereignty, however, the information management regime amendments must go far beyond those issues and beyond the *Privacy Act* and *Access to Information Act*. A system-wide review of Canada's information management regime is required. This paper has been prepared to assist First Nations as they press for change to the *Privacy Act* and associated legislation to better respect their rights. It also is intended to assist Canada by identifying areas for reform.

First Nations data sovereignty is an element of their inherent, Treaty, and constitutional rights to self-determination and self-government. First Nations data sovereignty means First Nations data is governed by First Nations laws. It incorporates the First Nations principles of OCAP® – ownership, control, access, and possession of data. Data is defined in this paper to mean information in any form:

1. About First Nations people like health, jobs, and housing;
2. From First Nations like languages, patterns, songs, dances; and
3. About First Nations reserve and traditional lands, waters, resources, and the environment.

The analysis presented here is a critical review of Canada's information management regime, highlighting systemic barriers to First Nation data sovereignty. These barriers include unilateral decision-making by the Crown, a conflict of values and the imposition of an individualistic regime and forced dependence on the private law of contracts to fill a gap in public law. More specific problems are also addressed, including:

- An over-collection of First Nations data and information, for which the Crown has been

chastised by the Auditors General four times since 2002;
- The sale of access to First Nations data by the Crown to third parties;
- A reliance on flawed consent provisions by the Crown to grant itself authority to use First Nations data at will;
- The use of First Nations data in a manner that sustains negative stereotypes; and
- The creation of roadblocks to First Nations access to their data and information.

This paper offers several suggestions for further exploration that may offer short-term and long-term improvements of the system. Three interconnected, multifaceted suggestions are offered. One addresses the colonialism inherent in the system, which means amending it to respect First Nations rights to self-determination and self-government as recognized by the Constitution, international commitments like the *United Nations Declaration on the Rights of Indigenous Peoples* and promises from successive Prime Ministers.

Another is the adoption of a multilateral system to engage First Nations decision-makers. A multilateral system is one that involves multiple decision makers, in this case Canada and the many First Nations, working cooperatively while respecting each other's laws, perspectives, and sovereign rights. In the short term, this might include pan-First Nations selected and operated review boards independent of, but embedded in, each federal department to oversee access, collection and publication of First Nations data held by the Crown. The long-term vision is Nation-based information management systems incorporating First Nations protocols, processes, and decisions about First Nations data.

A third suggestion addresses the Crown's presumptive ownership of First Nations data. Instead of owner, the Crown and First Nations can explore how Canada could instead serve as a steward or custodian of First Nations data. This simple shift of perspective would further support efforts to redress the inherent colonialism in the system.

In the short term, First Nations might enter into agreements with the Crown about how they wish their data to be stewarded. Over the longer-term, data repatriation and further enhancing First Nations data management capacity will ensure direct supervision by First Nations of their own data. A joint First Nation – Canada working group to dialogue on the separation of First Nations data from that legitimately owned by the Crown might be established to explore this complex question. The work of such a group might also support repatriation of First Nations data. This paper also echoes the Auditors General requirement that the Crown address its tendency to over-collect First Nations data. Finally, in the interest of building a just society, it is suggested the Crown respect its position as potential adversary in First Nations claims against the Crown by facilitating free, liberal, and timely access to First Nations data for claims research.

The conclusion of this paper is that it is the systemic impact of Eurocentric non-Indigenous concepts of privacy and ownership that impedes First Nations data sovereignty. The Crown assumes ownership of all First Nations data and information in its control and makes decisions about how to use, share, or dispose of that data through unilateral decision-making processes. Canada's information management regime is in breach of the Crown's moral and legal obligations to respect First Nations rights to self-determination and self-government. A system-wide, First Nations driven overhaul is required to accommodate First Nations data sovereignty premised on a Nation-to-Nation relationship. Multiple opportunities for improvement are identified. FNIGC encourages further discussion and refinement of the ideas presented herein to advance First Nations data sovereignty.

Introduction

The First Nations Information Governance Centre (FNIGC) is an incorporated, non-profit organization committed to producing evidence-based research and information that will contribute to First Nations in Canada achieving data sovereignty in alignment with their world views. The FNIGC is strictly technical and apolitical and is not a rights-holding organization. The FNIGC does not speak directly for First Nations. Mandated by the Assembly of First Nations' Chiefs-in-Assembly (AFN *Resolution #48*, December 2009), the mission of FNIGC is to strengthen First Nations data sovereignty and the development of information governance and management at the community level. We adhere to free, prior and informed consent, respect Nation-to-Nation relationships, and recognize the distinct customs of First Nations, to achieve transformative change. Our work includes research and analysis of the technical elements of First Nations data sovereignty, like information management.

The *Privacy Act*; *Statistics Act*; *Access to Information Act*; and the *Libraries and Archives Canada Act* make up the bulk of Canada's information management regime. This discussion paper highlights the challenges generated by Canada's information management laws hindering First Nations data sovereignty. First Nations data is information about First Nations people and their lands and waters. First Nations data sovereignty means their data and information is subject to First Nations laws. Data sovereignty is an element of First Nations rights to self-determination and self-government.

This paper begins with a discussion of the purpose of the information management regime, a brief history of its development in Canada, and notes the current reviews of the *Privacy Act* and *Access to Information Act* underway. The paper moves on to discuss First Nations data sovereignty – what it is, why it is important, and how it works. The two sections after that focus on the impacts of the regime on First Nations data sovereignty. Systemic problems are identified first. These include a system built on colonialism, a focus on individual privacy rights while denying First Nations collective rights, a failure to respect First Nations constitutional rights, the Crown's unilateral decision-making processes, and its presumption of ownership of First Nations data under its control.

The second section identifies more specific issues including:

- problematic definitions;
- over-collection of data from First Nations;
- failure to obtain free, prior, and informed consent for use of First Nations data;
- the sale of First Nations data to enrich the Crown and third parties;
- the distribution of anonymized First Nations data without consideration of the potential impact on First Nations;
- restriction of First Nations access to First Nations data;
- perpetual retention and public exposure of First Nations data unprecedented in the general population; and
- perpetuating stereotypes about First Nations in the interpretation and publication of First Nations data.

The paper concludes that Canada's information management regime poses a barrier to First Nations data sovereignty. This in turn impedes First Nations exercise of good governance to, among other things, improve their health and well-being and retain their languages and cultures. Data decolonization is part and parcel of First Nations demands that Canada respect First Nations rightful place in the federation.

Several suggestions to amend the system to better respect First Nations data sovereignty are presented in the final section of the paper for further exploration. This review is intended to provide

technical information on Canada's information management regime. It is not FNIGC's final position on the *Privacy Act*, or the broader legislative and regulatory landscape impacting First Nations data governance. This paper is intended to provide an opportunity for First Nations to learn more about Canada's information management regime, while engaging in dialogue to determine what changes are necessary to respect their data sovereignty.

First, this paper calls for the lingering vestiges of colonialism to be scrubbed from the legislation and its implementation. As will be seen, the legislation offends section 35 of the *Constitution Act, 1982*, numerous Supreme Court of Canada decisions, the *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP), and the recommendations of seminal reports on Crown-Indigenous relations. Sound legal arguments can be made that the regime is unconstitutional. Any amendments to the regime should respect First Nations role in the federation, promote reconciliation, embrace a Nation-to-Nation relationship, respect principles of free, prior, and informed consent, be based on the recognition of alternative legal orders, and be co-developed with First Nations. An amended regime should fully acknowledge and respect First Nations rights to self-determination and self-government and accord them the same respect as other governments.

Second, a new regime should embrace multilateralism. In a multilateral system parties agree to exchange and share data, while respecting each other's data sovereignty. A new system would be negotiated as equals and predicated on mutual trust and respect. First Nations would take over responsibility for decision-making regarding the Crown's access to and use of First Nations data currently under the Crown's control. This would support First Nations data sovereignty by replacing the Crown's unilateral management to one overseen by the rightful First Nations owners of the data. In the short-term, this might include pan-First Nation selected and operated data oversight review boards, embedded within every government institution and connected nationally. They would hold full decision-making authority over access to and publication of First Nations data held by the Crown. Their decisions would be binding on the Crown. As a gesture of good faith in a multilateral system, the Crown should cease the sale of First Nations data in any form and exempt First Nations from fees to access their own information.

Third, with a simple policy change respecting the Crown's relationship to the First Nations data in its possession, a new relationship of respect and due regard for First Nations data sovereignty could be launched. The Crown as steward or custodian of the data instead of owner of the data would allow a multilateral system to be initiated almost immediately, without even amending the legislation. For some First Nations, the Crown might serve as temporary steward or custodian of their data, while they work to repatriate their data and resume full data sovereignty. For others, a longer-term relationship could be negotiated. Agreements between the Crown and First Nations would spell out each party's duties and expectations. Nation-based data oversight review boards, like those already established by many First Nations would oversee implementation of the OCAP® principles as each nation sees fit. Government departments, particularly Indigenous Services Canada (ISC), Crown Indigenous Relations and Northern Affairs (CIRNAC), and Libraries and Archives Canada (LAC) would benefit from working with First Nations to develop new definitions, protocols, and processes for the collection, access, publication, retention, disposal, and repatriation of First Nations data, based on First Nations laws and in accordance with their interpretation of the principles of OCAP®. A joint federal – First Nation working group could be established to dialogue on identifying First Nations data as distinct from that legitimately owned by the Crown and to facilitate data repatriation. The Crown must fully address successive Auditors General's concerns about the over-collection of First Nations data. Finally, the Crown must also acknowledge its position as potential adversary in First Nations claims against the Crown and facilitate free, liberal, and timely

access to data in its possession by First Nations for claims research.

This review is intended to provide technical information on Canada's information management regime. It is not FNIGC's final position on the *Privacy Act*, or the broader legislative and regulatory landscape impacting First Nations data governance. This paper is intended to provide an opportunity for First Nations to learn more about Canada's information management regime, while engaging in dialogue to determine what changes are necessary to respect their data sovereignty.

Background on Canada's Information Management Regime

Privacy laws are crucial in protecting personal development of individuality, creativity, and autonomy; in protecting our human dignity, integrity, and identity; in alleviating stress in social interactions (Williams, 2011), and supporting democratic institutions (Cohen, 2013). Williams outlines the different kinds of privacy that exist. These include territorial privacy or privacy regarding a particular place such as the home; privacy of the physical body protected, for example, by laws that govern the medical profession; informational privacy pertaining to an individual's rights to control what information is released about them; and finally, privacy of communications such as mail, phone calls and doctor conversations (Williams, 2011). Friedewald adds three additional types of privacy: privacy of behavior and actions; privacy of data and images; and privacy of association (2013). Different kinds of privacy are protected by different kinds of laws (Williams 2011).

Privacy is a human right. Article 12 of the *Universal Declaration on Human Rights*, which Canada has endorsed, says,

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

A right to privacy was first recognized in 1977 as part of the *Canadian Human Rights Act* creating the Office of the Privacy Commissioner. A right to privacy is not included in the *Charter of Rights and Freedoms*, but the *Quebec Charter of Rights and Freedoms* includes rights related to privacy in sections 4, 5, and 9.

Privacy in dealings with the federal government is protected under Canada's information management regime. The regime has two primary objectives. The first is to protect personal and sensitive information held by the federal government, and the second is to allow all Canadians access to as much information held by the federal government as possible to foster transparency and accountability. This includes rights to access personal information about oneself and the right to correct that information if it is incorrect.

The advancements in digital networks and the Internet have created new challenges in protecting personal privacy. Now, more than ever, privacy can be violated without depriving someone of his/her/their freedom, without trespassing on property, or without having any contact with the person whose privacy is violated (Williams, 2011; Parliamentary Standing Committee on Access to Information, Privacy and Ethics, 2016a). We need only reflect on the power of the Internet to have a photo 'go viral' to know the truth of this. Recognizing the tremendous impact the digital revolution could have on personal privacy, the Organization for Economic Cooperation and Development (OECD) adopted a series of principles to protect personal information in the digital age (OECD, 1980). These principles were updated in 2013 (OECD, 2013). They have shaped the development of information management law and policy in Canada (Williams, 2011).

1. Accountability – an organization is responsible for data under its control.
2. Identifying – the purpose for which personal information is collected must be identified at the time of collection.
3. Consent – individuals must have knowledge of and consent to the collection, use, and disclosure of their personal information.
4. Limiting collection – only personal information that is necessary for the purpose of the organization may be collected except with consent of the individual.
5. Limiting use, disclosure, and retention – personal information is not to be used for other purposes except with consent.

6. Accuracy – personal information collected and stored must be correct.
7. Safeguards – security safeguards must be in place relative to the sensitivity of the information held.
8. Openness – organizations must make information available upon request about their policies and practices respecting data management.
9. Individual access – individuals can find out about the existence of, use and disclosure of their personal information and able to challenge its accuracy and completeness.
10. Challenging compliance – organizations must establish a process to address a complaint about their handling of personal information (OECD, 2013).

The federal government collects information in many ways for different purposes. For example, personal information is collected by the federal government every time you file a tax return, buy a train ticket, or use your passport. By virtue of the historic role and relationship between the federal government and First Nations, Canada collects even more information about First Nations individuals and communities – more than non-First Nations people (Goodman, 2018). For example, the federal government can only access non-Indigenous people's health records with a subpoena. In the case of First Nations receiving non-insured health benefits, however, the federal government has access to their medical records daily while approving payments. Information on First Nations education, housing, employment, and more is collected in different ways and in far greater amounts than is collected on any other Canadians.

In 2016, the Parliamentary Standing Committee on Access to Information, Privacy and Ethics studied the *Privacy Act*, first adopted in 1983 (Parliamentary Standing Committee on Access to Information, Privacy and Ethics, 2016a). The Report of the Committee identified three major themes for amending the legislation:

1. addressing technological changes;
2. modernizing the legislation; and
3. enhancing government transparency (Parliamentary Standing Committee on Access to Information, Privacy and Ethics, 2016b).

In response, the federal government undertook to conduct a review of the *Privacy Act*. (Minister of Justice, 2017). As part of that review, the Department of Justice (DOJ) issued a series of discussion papers on the *Privacy Act* inviting public comment (DOJ, 2019). Each of the first four discussion papers raise issues of relevance to First Nations data sovereignty. In addition, there is a fifth paper specifically on *Modernizing the Privacy Act's relationship with Canada's* [sic] *Indigenous peoples* (DOJ, 2019e). The federal government is also currently conducting a five-year review of the *Access to Information Act*.

FNIGC acknowledges the challenges with the *Privacy Act* identified by the Standing Committee and DOJ. To respect First Nations' data sovereignty, however, the information management regime amendments must go far beyond those issues and beyond the *Privacy Act* and *Access to Information Act*. A system-wide review of Canada's information management regime is required. First Nations participation in a multilateral system premised on respect for First Nations data sovereignty is essential when reconstructing Canada's privacy regime to protect everyone who lives within Canada.

First Nations Data Sovereignty

The term 'data' is defined here as more than just numbers and statistics that can be charted on a graph. It also includes stories, traditional knowledge, intellectual property, surveys, and research. 'First Nations Data' therefore is defined here to mean any information:

1. About First Nations people like health, jobs, and housing;
2. From First Nations like languages, patterns, songs, dances; and
3. About First Nations reserve and traditional lands, waters, resources, and the environment.

First Nations data sovereignty means all this data and information are subject to the laws of the First Nation. First Nations rights to data sovereignty extend to their citizens as individuals as well as their collective rights as nations and governments.

> *[T]he data governance rights of Indigenous nations apply regardless of where the data is held or by whom. This includes the right to the generation of the data that Indigenous peoples require to support nation rebuilding and governance... IDS (Indigenous data sovereignty) also comprises the entitlement to determine how Indigenous data is governed and stewarded (Raine, 2019).*

Data sovereignty is an element of self-determination and self-government. (Kukutai, 2016). Access to data and information about a nation's citizens, lands, waters, economies, natural resources, etc., is critical to good governance and sustainable development (United Nations, n.d., Office of the Privacy Commissioner, 2016). Without data and information, governments are unable to determine what policies and programs may be needed or the impact they might be having. Good governance requires reliable data and information. This is as true for First Nations as it is for the Government of Canada (Joint Advisory Committee on Fiscal Relations, 2019).

First Nations exercise data sovereignty through the application of their own laws, policies, and processes (FNIGC, 2020). How First Nations choose to exercise their data sovereignty is up to them. First Nations traditional laws and protocols, the modern application of these laws, and the need to develop new laws, codes, protocols, policies, and programs will influence First Nations individual data governance regimes. That said, First Nations have adopted a common approach to what constitutes data sovereignty. The OCAP® principles of ownership, control, access, and possession are individually and collectively the pillars of First Nations data sovereignty. These principles have been endorsed through the Assembly of First Nations (AFN) and trademarked by FNIGC for the collective benefit of First Nations. The ideas inherent in the First Nations OCAP® principles are not new. In fact, they represent themes and concepts that have been advocated for and promoted by First Nations people for years. Over the past two decades the First Nations principles of OCAP® have been successfully applied in dozens of First Nations across Canada. It's important to note that although there is a good degree of consensus surrounding OCAP®, each First Nations community or region may have a unique interpretation of the OCAP® principles. This is because OCAP® is not a doctrine or a prescription: it respects the right of First Nations communities in making its decisions regarding why, how, and by whom information is collected, used, or shared" (FNIGC, n.d.a.). In addition to their existing traditional laws and protocols, First Nations have established, for example:

- Privacy laws (Tsawwassen First Nation, 2009);
- Privacy policies (Mamalilikulla, 2020);
- Research review committees (Manitoba First Nations Health Information Research Governance Committee, n.d.);

- Data-sharing agreements like the Nova Scotia First Nations Client Linkage Registry (Tui'kn Partnership, n.d.a); and
- Standards to guide research and studies to ensure accuracy and cultural sensitivity (Assembly of First Nations Quebec and Labrador, 2014)

There is no room for dispute that First Nations have inherent, Treaty, and constitutional rights above and beyond those enjoyed by other Canadians (*Calder et al. v. Attorney-General of British Columbia*, 1973; *R.* v. *Sparrow*, 1990). These rights are protected under section 35 of the *Canadian Constitution, 1982*. While the specific rights are not described in section 35, Supreme Court of Canada decisions have provided some guidance regarding their content, as has the *United Nations Declaration on the Rights of Indigenous Peoples*. It is agreed that First Nations hold inherent and Treaty rights to self-government (*R.* v. *Pamajewon*, 1996; UNDRIP, Art. 4). The Crown must justify any infringement of First Nations constitutional rights (*R.* v. *Sparrow*, 1990). Government activity will be found by the Courts to infringe First Nations rights if it unreasonably interferes with First Nations rights, imposes undue hardship, or denies First Nations their preferred means of exercising their rights (*R.* v. *Sparrow*, 1990). Not all infringement of First Nations constitutional rights is contrary to section 35 and at times the Crown may be justified in limiting these rights. The infringement may be justified if it serves a valid legislative objective, there is as little infringement as possible, fair compensation is offered, and First Nations have been consulted or at least informed (*R.* v. *Sparrow*, 1990). The honour of the Crown is at stake in infringing First Nations rights and there must be no subterfuge or sharp dealing practiced by the Crown (*Haida Nation* v. *British Colombia*, 2004). The Crown's authority to infringe section 35 rights has been explored further in the multitude of cases that have followed on the duty to consult (i.e., *Haida Nation* v. *British Colombia*, 2004). It will become self-evident as this paper explores the impact of the regime on First Nations data sovereignty, that their constitutional rights are unjustifiably infringed.

The ambition of our vision, our goals, and our hearts when it comes to self-determination and holding Canada to our Treaty right, including the management and governance of our own data and information… we need to give voice to the people through ethical spaces and heal from historical harms created through unethical research practices created by colonization…Colonization and assimilation only interrupted our history. It's time we rewrite our own history and assert our sovereignty. (Chief Stanley Grier, First Nations Data Governance Strategy Summit, February 26, 2019)

Systemic Problems with the Information Management Regime

This section of the paper explores five elements of the existing information management regime that offend the principle of First Nations data sovereignty. It considers the implications of a system built on colonialism, the failure to accord respect in the regime to First Nations collective rights, lack of respect for First Nations governments, the issue of the Crown as unilateral decision-maker, and finally the reliance on private law of contracts to address the current public law failings.

Colonialism

Colonialism is a systemic problem that must be addressed in any amendments to Canada's information management regime. To colonize a people is to push them aside to occupy their lands, waters, and resources and impose the laws of the colonizer (Fanon, 1963). As will be seen, Canada's ongoing colonization of First Nations peoples and their territory is evident in the vast amount of data and information about and from First Nations people and lands that is claimed by Canada as its own and is made subject to Canadian law. A colonial perspective is found throughout the system – in the failure of Canada to acknowledge First Nations as governments and accord them the same respect as other governments, in the foreign system of law that places individual rights and interests ahead of the collective, and in the strong-arm tactics to obtain First Nations consent to use of their data. Additional examples are provided throughout this paper.

Colonization is not only morally repugnant (UNDRIP, Preamble), it is illegal under Canada's own laws (Borrows, 2019). With the adoption of section 35 of the *Constitution of Canada*, Canada recognized the inherent and Treaty rights of First Nations. Seminal reports, including the *Royal Commission on Aboriginal Peoples*, 1996, the *Report of the Truth and Reconciliation Commission*, 2015 and the *Final Report on the Inquiry into Missing and Murdered Indigenous Women and Girls*, 2019, highlight the impact of colonial policies on First Nations people. Canada has acknowledged its failures and has committed to a new approach.

> *This is a time of real and positive change. We know what is needed is a total renewal of the relationship between Canada and Indigenous peoples. We have a plan to move towards a nation-to-nation relationship based on recognition, rights, respect, cooperation and partnership, and we are already making it happen (Prime Minister Trudeau, 2015).*

DOJ has suggested modernizing the *Privacy Act* to include a specific objective of "advancing reconciliation with Indigenous peoples in Canada by promoting improved data sharing with Indigenous governments and communities" (DOJ, 2020). While broad statements of intent are a helpful assistance to the interpretation of the Act, they remain up to interpretation by the Crown.

The full endorsement of the *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP), and a commitment to incorporate its principles into Canadian law and policy (*Speech from the Throne*, 2020) are further evidence of a new approach. The federal government and the Province of British Columbia have adopted laws that require the application of UNDRIP federally and in BC (*Declaration on the Rights of Indigenous Peoples Act, 2021, and 2019 respectively*).

As noted earlier, the Supreme Court of Canada has recognized First Nations rights to self-government. This includes rights to data sovereignty. The specific need for First Nations data sovereignty was acknowledged by Canada in the *Report of the Joint Advisory Committee on Fiscal Relations* (Joint Advisory Committee, 2019). Addressing chronic underfunding for First Nations and closing the socio-economic gap to achieve the 2030 sustainable development goals demands First Nations have

access to data (Joint Advisory Committee, 2019). Recommendation 18 states:

> *The Committee recommends that sustained funding and attention be paid to supporting First Nations in their pursuit of data sovereignty, and ensuring respect for the principles of OCAP®. This will also require changes to federal legislation, institutions, policies, data holdings, and data practices to ensure alignment with OCAP®, including assigning a federal government body to monitor and enforce the compliance of federal departments and agencies [emphasis added] (Joint Advisory Committee, 2019).*

The Supreme Court of Canada has identified a duty on the Crown to consult with First Nations at the first instance the Crown contemplates activity that may infringe First Nations rights. The Crown therefore has a duty to consult with First Nations about any amendments to its information management regime. Recognizing First Nations rights draws on Supreme Court of Canada decisions about blending legal orders (Borrows, 2019). As noted in *Tsilhqot'in* v. *British Colombia*, "a morally and politically defensible conception of Aboriginal rights will incorporate both legal perspectives" (2014). Consultation will facilitate the incorporation of both Canadian and First Nations legal perspectives in the revised information management regime. Blending legal orders would anchor First Nations rights of data sovereignty to the bedrock of Nation-to-Nation relations.

Individual versus collective rights

While being cautious to respect diversity, there are some generalizations that can be made about common differences between First Nations perspectives and those of Canada. For example, many First Nations philosophies of interconnectedness explain their relationship to their lands, cultures, and each other, a relationship of belonging and responsibility that are different from the philosophy expressed by the Crown (*Royal Commission on Aboriginal Peoples*, 1996; Wilson, 2009). The concept of what is considered private is an additional example.

> *While 'private' information in mainstream discussions is commonly understood to include financial and health information, for Indigenous communities, 'private' information might include other types of information such as information associated with participation in ceremonies, hunting and gathering practices, or support for community development projects. Retaining privacy over certain traditional cultural practices is a long-established convention based on an understanding of collective privacy. There is a strong interest in preserving and reviving Indigenous languages, cultural practices, and value systems among Indigenous peoples and a resultant drive to have control over cultural heritage in a way that conforms with Indigenous laws and conventions (Gee, 2019).*

There also is a stark difference in perspectives held by First Nations and the Crown about the value of individual versus collective rights, including information management rights (Williams, 2011; Vis-Dunbar, 2011). On behalf of the Office of the Privacy Commissioner of Canada, the Informational Privacy Interdisciplinary Research Group (iPIRG) at the University of Victoria, BC explored the issue of collective rights to privacy. They concluded that the Crown's preference for individualism is evident in the information management regime. "Community interests are not mentioned explicitly, leading one to infer that a community's privacy interest is seen under Canadian (statutory) law as being reducible to the privacy interests of its members" (Vis-Dunbar, 2011). In other words, groups are treated as a collection of individuals. Any group rights to privacy are only those enjoyed by them as individuals, whether they be humans or corporations. Therefore, under the Canadian regime, First Nations citizens have individual rights to privacy of their personal information. These are the same rights enjoyed by all Canadians. First Nations do not however hold a collective right to privacy. While it is important that Canada respect First Nation individual's privacy in

their information management regime, it is equally important that Canada recognize First Nations collective rights to privacy and data sovereignty.

It is settled law that First Nations have collective rights (*Behn* v. *Moulton Contracting Ltd.*, 2013). It is argued here that First Nations are owed a collective right to privacy beyond the rights of First Nations citizens to their individual privacy. First Nations are first and foremost Nations and are owed that respect in keeping with the *Royal Proclamation, 1763* (*Calder et al.* v. *Attorney-General of British Columbia*) and subsequent legal developments in Canada (Borrows, 2019). UNDRIP recognizes and affirms 'that [I]ndigenous peoples possess collective rights which are indispensable for their existence, well-being, and integral development as peoples" (UNDRIP, Preamble). It identifies several collective rights, including rights to self-government. First Nations are fully empowered governments with authority to manage their own affairs (UNDRIP, Art. 4). The Prime Minister has committed to a Nation-to-Nation relationship (Trudeau, 2015; 2020).

There is growing recognition that individual rights are not adequate for the purpose of protecting First Nations collective rights to privacy (Vis-Dunbar, 2011). This has been acknowledged by the federal government, "[s]ince individual and communal Indigenous privacy interests can be deeply intertwined, this raises the question of whether the *Privacy Act* could reflect the unique concept of communal privacy interests" (DOJ, 2020). One possible approach to address this problem is to develop a groups' rights model of ownership of data and information (Vis-Dunbar, 2011). This may entail developing a new common law concept of group rights. This route relies on the Courts, it is expensive, time consuming, and its outcome entirely uncertain. There is a far simpler and faster solution, which is to recognize the collective rights of First Nations as nations. Amendments to the information management regime would embed a Nation-to-Nation relationship simply through the Crown's recognition of all First Nations as governments to be treated in like manner to other international, provincial, and municipal governments.

Lack of recognition of First Nations governments

The Canadian information management regime does not currently recognize most First Nations collective rights to privacy and data sovereignty. As will be seen, only a small handful of First Nations governments are currently accorded the same treatment as other governments under the legislation. For example, section 13 of the *Access to Information Act*, stipulates that the Crown may not share information received from another government.

> 13 (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Part that contains information that was obtained in confidence from
>
> (a) the government of a foreign state or an institution thereof;
>
> (b) an international organization of states or an institution thereof;
>
> (c) the government of a province or an institution thereof;
>
> (d) a municipal or regional government established by or pursuant to an Act of the legislature of a province or an institution of such a government; or
>
> (e) an Aboriginal government.

While part (e) looks like generous recognition of First Nations rights, in fact, an 'Aboriginal Government' is narrowly defined in the legislation (s.13(3)). It only includes the following Indigenous governments,

> (a) Nisga'a Government, as defined in the Nisga'a Final Agreement given effect by the *Nisga'a Final Agreement Act;*
>
> (b) the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the *Westbank First Nation Self-Government Act*;
>
> (c) the Tlicho Government, as defined in section 2 of the *Tlicho Land Claims and Self-Government Act;*

(d) the Nunatsiavut Government, as defined in section 2 of the *Labrador Inuit Land Claims Agreement Act;*
(e) the council of a participating First Nation as defined in subsection 2(1) of the *First Nations Jurisdiction over Education in British Columbia Act*;
(f) the Tla'amin Government, as defined in subsection 2(2) of the *Tla'amin Final Agreement Act*;
(g) the Tsawwassen Government, as defined in subsection 2(2) of the *Tsawwassen First Nation Final Agreement Act;*
(h) the Cree Nation Government, as defined in subsection 2(1) of the *Cree Nation of Eeyou Istchee Governance Agreement Act* or a Cree First Nation, as defined in subsection 2(2) of that Act;
(i) a Maanulth Government, within the meaning of subsection 2(2) of the *Maanulth First Nations Final Agreement Act;*
(j) Sioux Valley Dakota Oyate Government, within the meaning of subsection 2(2) of the *Sioux Valley Dakota Nation Governance Act*; or
(k) the council of a participating First Nation, as defined in section 2 of the *Anishinabek Nation Education Agreement Act*.

Likewise, Sections 8 and 19 of the *Privacy Act* identify specific First Nations that will be treated like other nations and governments. Even this degree of respect is not applied across the board for the First Nations listed. Note for example, First Nations in Ontario are 'governments' with respect to their education data, implying that with respect to all other data they are not considered a government by Canada. While these First Nations are to be applauded for winning concessions from the Crown, it simultaneously denies all other First Nations governments equivalent status. This creates classes of First Nations governments, winners and losers in respect of their rights. Moreover, it requires First Nations to fight for recognition as governments when every other national government, groups of nations like the North Atlantic Treaty Organization (NATO), and subdivisions of nations including even municipalities are automatically respected as governments. There is a long-standing principle of recognition of the privacy rights of sovereign nations and other governments to respect the collective rights exercised by governments (United Nations, 1945). Canada applies this principle in its information management regime for most governments except First Nations.

It is a fact of law that the *Indian Act* established Indian Bands as wards of the state, to be supervised by the Crown in the exercise of limited authority delegated to them under the *Indian Act* by the Ministers of ISC and CIRNAC (*Guerin* v. *The Queen*, 1984; First Nations Studies Program, 2009). By this logic, Indian Act Bands, which make up most First Nations governments in Canada, are not self-determining or self-governing, have no independent power or authority and are not in fact Nations. They are instead administrative bodies of the federal government. There is internal logic to this system, yet it entirely sidesteps the fact that *the Crown itself stripped First Nations of their rights to self-determination and self-government and imposed the Indian Act in the first place as a means of colonial domination*. The information management regime is not a system built on logic, but instead built on the historic abuse of First Nations collective rights. The colonial *Indian Act* regime cannot be used to justify the infringement of First Nations collective rights to data sovereignty. Failure to accord First Nations governments similar respect as all other governments because the Crown refuses to acknowledge them as such, constitutes a systemic denial of rights of First Nations governments.

First Nations are distinct and equal partners in confederation, not wards of the state subject to unilateral decision-making by a colonial government. They hold inherent and Treaty rights to self-government and deserve respect like other governments. Canada has begun to acknowledge its failures to respect First Nations rights but has a long way to go yet to dismantle the colonial system and welcome First Nations as rightful partners in confederation (Borrows, 2019). The 2020 DOJ discussion paper on the *Privacy Act* notes the need

for a new "definition of "[A]boriginal government" with a more flexible definition that reflects the diversity of Indigenous governance models" (DOJ, 2020). Questions remain about exactly what DOJ might propose in this regard.

Unilateralism versus multilateralism

At present, the Crown pursues a unilateral approach to First Nations data management. This paper defines a unilateral or 'stove pipe approach,' as one where a single entity is gatekeeper, makes all decisions about the use, collection, storage, sharing, and destruction of the data and information, and facilitates public access to and reporting on the data and information. This generally describes Canada's relationship to First Nations data and information. Although Canada has many different government departments, which may not always act in unison and often function independently, they are one unified structure *viz-a-viz* First Nations. The federal departments, collectively operate a unilateral system.

As will be seen in the section on specific problems with the information management regime below, the Canadian information management regime dictates how and what data will be collected by the Crown, the Crown has sole decision-making authority over who has access to the data, when and how data will be shared, and how it will be disposed of or destroyed. For example, subsection 8(2)(b) of the *Privacy Act* allows the Crown to make public any personal information, "for any purpose in accordance with any Act of Parliament or any regulation made there". The *Statistics Act* creates and outlines the duties of Statistics Canada. Its responsibilities are to,

(a) to collect, compile, analyse, abstract and publish statistical information relating to the commercial, industrial, financial, social, economic and general activities and condition of the people;
(b) to collaborate with departments of government in the collection, compilation and publication of statistical information, including statistics derived from the activities of those departments;
(c) to take the census of population of Canada and the census of agriculture of Canada as provided in this Act;
(d) to promote the avoidance of duplication in the information collected by departments of government; and
(e) generally, to promote and develop integrated social and economic statistics pertaining to the whole of Canada and to each of the provinces thereof and to coordinate plans for the integration of those statistics.

As further evidence of Canada's unilateral approach, note the duties of the Chief Statistician, who shall,

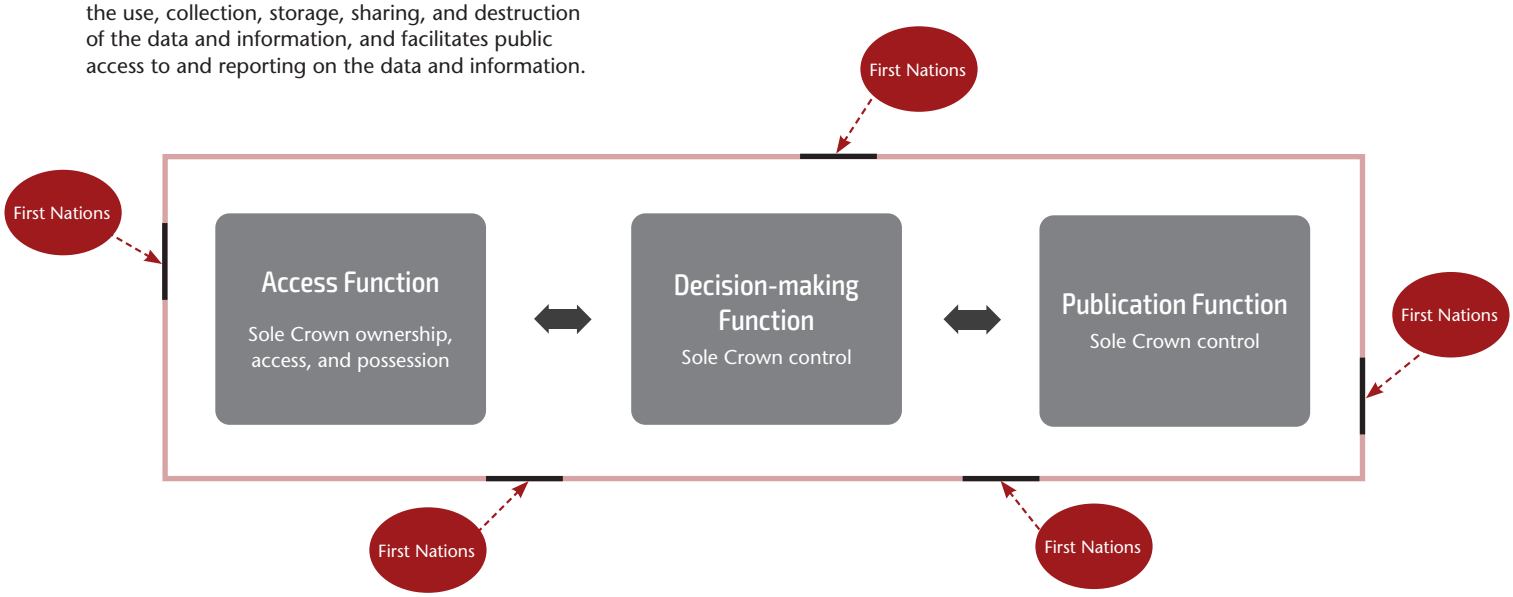
(a) decide, based strictly on professional statistical standards that he or she considers appropriate, the methods and procedures for carrying out statistical programs regarding
  (i) the collection, compilation, analysis, abstraction, and publication of statistical information that is produced or is to be produced by Statistics Canada,
  (ii) the content of statistical releases and publications issued by Statistics Canada, and
  (iii) the timing and methods of dissemination of statistics compiled by Statistics Canada;
(b) advise on matters pertaining to statistical programs of the departments and agencies of the Government of Canada, and confer with those departments and agencies to that end; and
(c) control the operations and staff of Statistics Canada (ss. 4(5) *Statistics Act*).

There is no need to engage with First Nations in this legislation or to consult with them. It is the Chief Statistician who holds sole decision-making authority about what information on First Nations to release to the public. The legislation also created a Canadian Statistics Advisory Council (s 8.1), but it is, as the name suggests, purely advisory. The members are appointed by the Crown and serve at the Crown's pleasure. At the time of writing, one First Nation person sits on the Council (Innovation, Science, and Economic Development Canada, 2019). First Nations were not consulted on the creation of the

legal regime in the first instance, and for the most part the system functions without any form of First Nations engagement, consultation, or oversight.

Figure 1 below is a representation of Canada's unilateral system. In this paper, the *Access Function* is defined here as the physical storage and retrieval of the data. The *Decision-making Function* refers to the exercise of decision-making over the collection, use, sharing, research on, manipulation, disposal, and archiving of data. The Decision-making Function approves requests to access and publish information. The *Publication Function* refers to the presentation of data and information in reports, statistics, discussion papers, speeches, etc. In a multilateral system parties agree to exchange and share data, while respecting each other's data sovereignty. A multilateral approach divides up these areas of concern, separating responsibilities to accommodate the jurisdiction of multiple parties. In computer science this is referred to as 'separation of concerns' (Dijkstra, 1982). The various parts of the system can speak to one another, but they hold different authorities. It allows the appropriate sharing of data, without compromising the security of the data or losing sovereignty in the data. The international standard "supports distribution, interworking, portability, and platform and technology independence" (emphasis added) (SO/IEC 10746-3, 2009). The Open Geospatial Consortium uses this as its computer data interface standard (Open Geospatial Consortium, 2015). The *INSPIRE (Infrastructure for Spatial Information in Europe) Architecture and Standards Position Paper*, provides a useful model of this multilayered process (INSPIRE, 2002). It has been simplified here to show the contrast with the unilateral system.

Figure 1: Unilateral Data Decision-making
A single entity is gatekeeper, makes all decisions about the use, collection, storage, sharing, and destruction of the data and information, and facilitates public access to and reporting on the data and information.

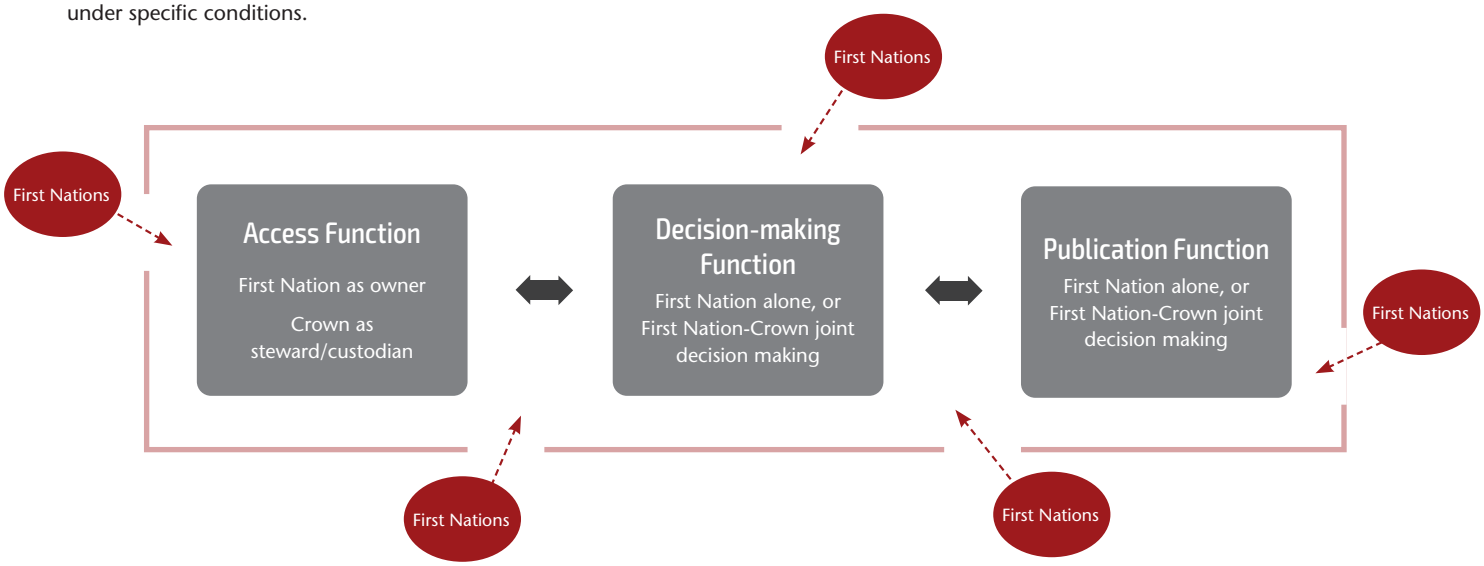


A multilateral system supports data sharing between sovereign states. See for example the *Memorandum of Understanding between the Department of Citizenship and Immigration of Canada and the Canada Border Services Agency and the Department of Immigration and Border Protection of the Commonwealth of Australia Regarding the Exchange of Information* (2016) and others like it (Immigration, Refugees, and Citizenship Canada, 2018). This *Memorandum of Understanding* deals with sharing information to track the migration of people between Canada and Australia (Article 1). It includes provisions on what the information can be used for and whether

it can be shared with others (Article 3), who has access to the information (Article 8), and the retention and disposal of the information (Article 9). Neither party has suspended its sovereignty in favour of the other. Each retains authority to store, access, use, share, and publish their own information under their own domestic laws but agrees to share it with another sovereign state under specific conditions. Although this example is at the international level, it can be applied in the context of the Nation-to-Nation relationship between Canada and First Nations.

Figure 2: Multilateral Decision-making System

Each state retains authority to store, access, use, share, and publish their own information under their own domestic laws but agrees to share it with another sovereign state under specific conditions.



> *In terms of the nation-to-nation relationship, reciprocal accountability is the key goal. This means that each partner is accountable for the actions and effective implementation and operation of their systems, ensuring that the partners are simultaneously independent and interconnected (Nickerson, 2017).*

The current unilateral system operating in Canada with respect to First Nations data is a remnant of the colonial era and needs revision. John Borrows, Canadian Research Chair in Indigenous Law, notes, the "existence of multiple sources and sites of power in Canada goes some distance toward repudiating a single-source origin story that places all authority in the Crown" (Borrows, 2019). A revised system must give due regard and respect to the principles of data sovereignty accorded by the Crown to other governments and embrace a multilateral approach to data sharing. DOJ has acknowledged the need for new mechanisms and tools to address "communal privacy interests", but no information on those have been shared by the Crown at the time of writing (DOJ, 2020).

Private law to address public failings

One final systemic issue must be raised here. This is the reliance that First Nations have had to place on the use of private law solutions like contracts to address the problems with the federal public law information management system.

Contracts that address the collection, storage, use, access to, publication of, and/or disposal of data are a mechanism that is currently available to provide some degree of protection for First Nations and

their data. There are several examples of contracts or agreements between First Nations and the federal and provincial Crowns and/or third-party data management organizations. This includes,

- the tripartite arrangement between the federal government, BC provincial health authority and the BC First Nations Health Council (First Nation Health Authority, 2011),
- the agreement between the Chiefs of Ontario and ICES (Institute for Clinical Evaluative Sciences) (Pyper, 2018), and
- the Tui'kn Partnership between five Mi'kmaq communities in Cape Breton, Nova Scotia, Nova Scotia Department of Health and Wellness, and Health Canada (Tui'kn, n.d.).

In these cases, the First Nations have negotiated contracts with federal, provincial, and/or private sector institutions to steward their health data on behalf of the First Nation. FNIGC acknowledges with respect, the considerable work that went into negotiating and implementing these agreements and encourages their use as a temporary stop gap measure. They allow First Nations to take some measure of jurisdiction over their data. However, these agreements remain subject to and can be trumped by legislation and common law. They are essentially a private law effort to address a failure of public law to respect First Nations data sovereignty. A reliance on private contract law is not a sustainable or acceptable substitution for constitutional rights.

Thus far the paper has identified several systemic problems with the Canadian information management regime. This includes a failure to respect First Nations governments, a unilateral decision-making process controlled by the Crown, and a failure to accord First Nations their collective constitutional rights. This has forced First Nations to rely on private law to address failings in the public law system. Overall, the system is colonial in nature and effect.

Specific Problems with the Information Management Regime

Having completed an exploration of some general themes for information management reform, this next section explores the system in greater depth to expose additional impacts on First Nations' data sovereignty. Highlighted below are specific problems with definitions, collection, consent, the use, sharing, control, possession, access, retention, disposal, and publication of First Nations data and information.

Definitions

As part of its review, the Department of Justice has identified a need for new definitions to improve the interpretation and application of the *Privacy Act*. This includes amendments to existing terms like 'personal information' or adding new definitions like 'publicly available personal information' (Department of Justice, 2019c). This section will look at some selected terms used in the legislation that present complications for First Nations data sovereignty.

The phrase 'consistent use' is a problem in the *Privacy Act*. As a rule, the *Privacy Act* requires personal information only be used for the purpose it was collected in the first place (section 4). However, section 8 of the *Privacy Act* also allows the use of personal information in a fashion considered to be "consistent" with the use it was to be originally put. There is no need to obtain further consent for these new additional uses of the data. The Supreme Court of Canada test for identifying a valid consistent use is that it,

> *need not be identical to the purpose for which [the] information was obtained in order to fall under s. 8(2)(a) of the Privacy Act; it must only be consistent with that purpose. There need only be a sufficiently direct connection between the purpose and the proposed use, such that an [individual] would reasonably expect that the information could be used in the manner proposed (Bernard v. Canada (Attorney General), 2014).*

This statement from the Supreme Court is problematic in the First Nation context. It is vague and leaves a great deal of room for interpretation. Sadly, given the Crown's practices of using and disclosing First Nation information without First Nation consent, First Nations have learned that they can "reasonably expect" their information to be used for ANY purpose in ANY manner. Surely the historic and ongoing abuse of First Nations data and information cannot be considered 'consistent use' or the legal standard to apply. The low standard of privacy accorded by the Crown to First Nations must not regulate the interpretation of the phrase 'consistent use.' DOJ has flagged the vague language has been problematic for federal officials in defining the term (DOJ, 2020). Further discussion is warranted to ensure that a revised Act meets the needs of the Crown as well as those of First Nations.

'Necessity' is another problematic term. The Office of the Privacy Commissioner of Canada has recommended the need for a definition of 'necessity' to curb the over-collection of information (DOJ, 2019a). The argument being that each department must be able to show how 'necessary' it is for the information to be collected to run their programs and projects. The Crown struggles with this issue. Successive Auditors General gave the federal government failing grades on its over-collection of First Nations data and information in 2002, 2006, 2011, and in 2018 (Office of the Auditor General, 2002, 2006, 2011, and 2018). They found that the Crown's data collection was insufficient in some areas and overabundant in others. Overall, the Crown fails to adequately use the information already in its possession. Clarifying the Crown's duty is helpful, but for First Nations, it does not address the issue of data sovereignty. A judgement call by the federal government alone as to what is necessary – even with clarification – merely extends a habit of unilateralism and a bureaucratic culture that equates voluminous reporting with productivity. If Canada were to instead respect First Nations data sovereignty, the Crown alone would not determine

how much information it requires. Instead, it should seek permission from the First Nations, who would assess Canada's request for data according to First Nations laws and protocols and grant or deny this request accordingly. This would ensure that First Nations rights to self-government and self-determination are respected and adhered to in implementation.

The Department of Justice (DOJ) has further suggested a 'reasonable and proportional' principle to be included in Canada's information management regime, that "would aim to place a contextually sensitive, holistic and balanced approach to privacy impact and risk minimization at the heart of an institution's decision-making" (DOJ, 2019a). As stated previously, however, leaving it solely in the hands of the Crown to make these kinds of judgements does not address First Nations data sovereignty. As overarching principles, the recommendation for contextual sensitivity, holism, and balance are welcome. These are principles found in many Indigenous cultures, including First Nations (UNEP, 1999). Many First Nations have operated from these principles since time immemorial. As these are new principles to the Canadian regime, working with First Nations who have more experience with this approach is a learning opportunity for all involved. These principles have the potential to enrich Canada and First Nations in their various, independent, but interconnected information management regimes.

Another problematic phrase is the 'public interest.' Subsection 8(2)(m)(i) of the *Privacy Act*, is open to wide interpretation. This section allows the Crown to use First Nations data and information in the public interest where the "disclosure clearly outweighs any invasion of privacy that could result from the disclosure.' Unfortunately, what is 'in the public interest' for the Crown may be cause for suffering by First Nations. Pipelines, ski resorts, hydro dams and more have been deemed to be in the 'public interest' (*Delgamuukw* v. *British Colombia*, 1997, para 165). Even the principles of reconciliation and social harmony have been proposed as justification to infringe on First Nations rights in the majority decision by Chief Justice Lamar in *R.* v. *Gladstone* (1996, para 73-75). Justice Beverly McLachlin, noted in her dissent in *R.* v. *Van der Peet* that such an approach is ultimately more 'political than legal' (1996, para 302), meaning that the Chief Justice was putting the provincial government's political interests ahead of First Nations legal rights. Justice McLachlin went on to become the Chief Justice and had an opportunity to address this issue in the decision recognizing Tsilqhot'in Aboriginal land title. The Judge in the original lower court decision upholding Tsilqhot'in title described the problem quite well.

> *The majority's link between it's [sic] theory of reconciliation and the justification of infringements test described in Van der Peet and Gladstone would appear to effectively place Aboriginal rights under a Charter s. 1 analysis. As McLachlin J. points out, this is contrary to the constitutional document, and arguably contrary to the objectives behind s. 35(1). The result is that the interests of the broader Canadian community, as opposed to the constitutionally entrenched rights of Aboriginal peoples, are to be foremost in the consideration of the Court. In that type of analysis, reconciliation does not focus on the historical injustices suffered by Aboriginal peoples. <u>It is reconciliation on terms imposed by the needs of the colonizer</u> [emphasis in the original]. (Tsilhqot'in Nation v. British Columbia, 2007 BCSC 1700).*

The interpretation of terms like 'in the public interest' currently is exercised by a majority non-Indigenous public service which is mostly ignorant of First Nations' perspectives, interests, or rights. Most civil servants are simply unequipped to make an appropriate judgement call on how First Nations data and information can appropriately be used in 'the public interest' that does not do further damage to First Nations. Hiring Indigenous people to the federal public service is not the solution, because the decision-making must come through the First Nation governments. In any case, this

should not be an issue of discretion by the Crown and its civil servants but of discussion with First Nations in full recognition of their rights, including data sovereignty.

DOJ has proposed removing the current public interest provision (ss 8(2)(m) of the *Privacy Act*) and replacing it with

> *a new framework that could permit a further use or disclosure of personal information for a purpose not specifically identified in the Act where the head of a federal public body determined that doing so would be "reasonably required" in the public interest, with an associated record-keeping requirement for such decisions to allow review by the Privacy Commissioner... [T]he Act could identify key considerations that the head of a federal public body would have to take into account in determining whether another use or disclosure was "reasonably required" (DOJ, 2020).*

This additional guidance might be helpful to assist federal officials in determining what is in the public interest.

There is potential for this clause to serve as a means for First Nations to access personal information for purposes other than under agreement (subsection 8(2)(f)), for research (ss (j)), or for claims research (ss. (k)). Subsection 8(2)(m) is little used, however, because few proposals to access personal data under this provision pass the "invasion of privacy test" (TBS, 2010) and would likely not withstand a Charter challenge.

Collection

First Nations are one of the most studied groups in Canada (Goodman, 2018). Colonial governance has meant vast quantities of data and information about First Nations' citizens, lands, and waters are collected, far beyond what is expected of non-Indigenous Canadians. The Auditors General have been highly critical of the federal government many times in this regard.

> *In 2002, we looked at the amount of reporting required of First Nations by federal organizations. We estimated that four federal organizations together required about 168 reports annually from each First Nations reserve. We found that many of the reports were unnecessary and were not in fact used by the federal organizations. We followed up on this issue in 2006. At that time, we found that federal departments had made little progress on meeting our recommendations to reduce reporting requirements. In our 2006 follow-up audit, we reported that INAC's officials told us that the Department obtained more than 60,000 reports a year from over 600 First Nations communities. The Treasury Board of Canada Secretariat analyzed the extent of federal involvement with First Nations and confirmed the seriousness of the problem we had identified in 2002 (Auditor General of Canada, 2011).*

As earlier mentioned, the federal government received another failing grade on First Nations data collection and management in 2011 and again in 2018. This leads to the conclusion that the Crown does not know how to address the problem or lacks the political will to do so.

The Crown regularly collects more information than strictly necessary or permitted by the legislation. For example, the *Indian Act* section 5 and other sections, allow the Crown to hold the following information in the Indian Register: name, date of birth, date of registration, band, and parents. However, significantly more information is collected, including information on marriages, divorces, children, adoptions, siblings, residence, and much more. More information collected means more information that is open to abuse. Technically, the legislation only allows for collection of information with a sufficient connection to legally authorized programs and projects.

Limiting the collection of personal information is one of the key principles of privacy and information management noted at the very beginning of this

paper. But, as the Auditors General have pointed out for almost twenty years, too much information on First Nations is being collected and little of it is used. There is no specific authority for this extra collection. Indigenous Services Canada (ISC) clearly takes a permissive approach to information collection. The list of data banks on First Nations held by ISC alone includes education, governance, entrepreneurship, social and community development, infrastructure and capacity, Aboriginal rights and interests, Residential Schools resolution, and First Nations individual affairs (ISC, 2015). ISC would be hard pressed to explain how all this information is 'necessary' or 'reasonable and proportional.' This collection of information is connected to issues of sovereignty, even beyond First Nations data sovereignty and are worthy of more discussion than is possible here. For now, however, it can be stated categorically that this practice of over-collection does little to build trust or generate momentum towards First Nations data sovereignty. DOJ has suggested a revised Act would include a more contextual approach to assist federal public bodies in determining whether their requests for information are necessary and reasonable (DOJ, 2020). These proposals will have to be considered in light of the Auditors General reports on over-collection of First Nations data.

Problematic as well is that a large amount of First Nations information is collected indirectly from First Nation administration and other service providers. There is no legal authority for the indirect collection. For example, much of the Indian Register information is collected by Indian Register administrators (IRA) that are employed by each First Nation. The IRAs collect the information and submit it to the Crown. ISC requires the IRA to sign an oath of confidentiality in favour of the Crown, as against the IRA's employer, the First Nation. This puts the IRAs in a difficult conflict of interest position. The information collected for the Non-Insured Health Benefits is also collected indirectly. First Nation and other health service providers and pharmacists submit the information to the federal government via the First Nations Inuit Health Branch at ISC.

This gives ISC direct access to personal information about the health of First Nations individuals without seeking their consent directly. The presumption is that those who collect the data in the first place have obtained consent. Education, employment, and housing information are likewise collected by service delivery organizations who administer federally funded programs in these fields on behalf of the Crown.

Further, Statistics Canada is empowered to enter into agreements with provinces, other government departments, municipalities, and corporations to collect information for statistical purposes (see sections 10, 11, and 12) which further expands collection of First Nations data by third parties on behalf of the federal government. This raises questions about whether the Crown is adequately meeting its fiduciary duty in these cases and where responsibility for transparency and accountability lie when a third party collects the information on behalf of the Crown. A reliance on data security systems of third parties brings into question the capacity of the Crown to meet its legal obligations to protect First Nation individual's privacy.

DOJ is considering expanding the capacity of the Crown to access data indirectly. This might include:

- where the individual provides consent to indirect collection of their personal information;
- where the information is "publicly available" and is being collected for a purpose other than making a decision directly affecting the individual;
- where collection from another source is authorized or required under another act of Parliament; or
- where the information is received from another federal public body pursuant to a disclosure authorized under the *Privacy Act* (DOJ, 2020).

These new provisions may further exacerbate First Nations concerns about indirect

collection and appear to offer little benefit in advancing reconciliation.

In addition, FNIGC is aware of the Crown making unreasonable demands on First Nations in collecting First Nations data and information. For example, in many contribution agreements like the one noted below, First Nations are required to grant the Crown an unlimited license to exercise "all intellectual property rights" that arise "for any Crown purpose." This provision requires First Nations to surrender their capacity to control the use of their intellectual property rights. This is another example of how the Crown imposes economic deprivation on First Nations. The ISC 2020-2021 *Comprehensive Funding Agreement (with 10-year grant) 2020-2021* (Funding Agreement) is an example. Note that '[/:Name]' refers to the First Nation or Tribal Council party to the agreement.

> *29 Intellectual Property*
>
> *29.1 All intellectual property that arises out of or under this Agreement will be owned by [/:Name] or a third party as may be set out in an agreement between [/:Name] and such third party.*
>
> *29.2 [/:Name] hereby grants to Canada a non-exclusive, royalty-free, fully-paid, perpetual, worldwide, and irrevocable licence to exercise all intellectual property rights that arise under this Agreement for any Crown purpose.*
>
> *29.3 [/:Name] shall secure all necessary rights to give effect to the licence granted under this Agreement.*

While some First Nations and First Nation organizations have managed to negotiate less egregious language most of the First Nations sign the funding agreement as is. Perhaps out of fear they will lose their funding if they reject this clause.

Consent

It is undeniable there is a power imbalance between the people and the Crown. Take for example filing one's taxes. Those who earn an income must file a tax return every year by a certain time, in a prescribed form, with a great deal of highly personal information. This is mandatory. Most Canadians file their taxes because of the threat to their wallet and freedom if they do not. This power of the state is why the Crown needs to be circumspect in its operations.

Nowhere is this power imbalance as stark as between First Nations' citizens and the Crown, and it takes on a different flavour for First Nations than it does for most Canadians. As First Nations have learned from history, the Crown's demands are not to be trifled with, because not meeting those demands results in serious consequences. We have seen through the *Royal Commission on Aboriginal Peoples* (RCAP, 1996), *Report of the Truth and Reconciliation Commission* (2015) and the *Inquiry on Missing and Murdered Indigenous Women and Girls* (2019) the consequences of systemic abuse of power by the Crown. These experiences have affected the way many First Nations citizens engage with the Crown; not with respect, but with fear. For many First Nations, agreeing to the Crown's demands is acquiescence under threat, real or perceived. Fear of consequences should not be mistaken for consent.

Consider First Nation people registering for status. As noted above, they are required to submit more information than the legislation contemplates, and they are required to agree to a host of other conditions for the use of the information far beyond registration (ISC, 2020). Of course, First Nations citizens are free to withhold their consent by not submitting the form. As a result, though, they will not be considered for Indian status registration. This can affect employment, education, and housing, in addition to negatively impacting family and community bonds, and even the legal right to reside in their own community. Even if a First Nation person is comfortable with submitting excessive information for the purpose of Indian status registration, there is no legal obligation on the Crown to obtain their further consent for other uses of their personal information. This includes all the exceptions contained in Article 8(2) of the *Privacy Act*, like research and statistical analysis by Canada or

third parties. Where the option is to submit the data and information or be denied a service or benefit that has nothing to do with any further use of the data and information, the concept of consent is challenged. These zero-option measures mean there is no consent – merely acquiescence in the face of a bully. This certainly does not meet the standard of 'free, prior, and informed consent', outlined in the *United Nations Declaration on the Rights of Indigenous Peoples*.

DOJ has suggested that the "Act could include factors or standards to help ensure that individual consent provided under the Act is specific, informed, and voluntary, and able to be revoked" (DOJ, 2020). FNIGC notes, that Bill C-11 *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, which received first reading in the House of Commons on November 17, 2020, subsection 15(5) states,

> *The organization must not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of their personal information beyond what is necessary to provide the product or service.*

A similar provision to be included in the *Privacy Act* could be explored to address First Nations concerns about consent provisions and practices.

Use of First Nations data

The Crown makes use of First Nations data and information when, how, and for what purposes it chooses, without the engagement of First Nations and under dubious consent provisions. This section looks at the use of 'anonymized' data and the sale of First Nations data by the Crown. It also describes and reflects on the use of personal information banks, which are descriptions of data held by the federal government.

Anonymized or de-identified data is information that has been stripped of personal details, so it is not possible to identify individuals to whom the data applies (Rocher, 2019). For example, the Canadian census conducted by Statistics Canada gathers a great deal of personal information including name, race, religion, income, housing, etc. The *Privacy Act* includes this information in its definition of 'personal information' that cannot be shared with the public. To make use of the information in the census without being in breach of the *Privacy Act*, Statistics Canada strips away the personal information and instead looks at the aggregated data. This data has been anonymized and can now be made public. The Crown can use the information for its own purposes, as well as provide it to the public directly or under an access to information request.

It is a great system when looking at a population the size of Canada, roughly 37 million (Statistics Canada, 2020a). The total estimated First Nations population is about one million (Statistics Canada, 2019a). As a result, when First Nations' data is separated from data concerning others, the First Nations' data becomes less anonymous. In some communities the populations are so small it would be easy to identify individuals from so called anonymized data. Even if First Nations anonymized data is broken out by larger groupings, there are so few communities in some provinces that it would be easy to determine what community the data identifies. This could expose an entire community to prejudice. Statistics Canada has policies to suppress some data, which limit disclosure of personal information (Statistics Canada, 2019b). Researchers have concluded, however, that it is possible to de-anonymize data (Rocher, 2019). The use of anonymized data therefore raises serious questions about the protection of First Nations' rights to privacy and the capacity of the Crown to prevent a breach of these rights.

Statistics Canada's Research Data Centres hold microdata and are located at 32 universities across Canada as well as three in Ottawa (Statistics Canada, 2020b). University, government, and private sector researchers may access these data banks under specific terms and conditions, including

confidentiality. In some cases, these researchers are permitted access to the un-anonymized data to create data linkages, which involves combining different data sets to learn something new. Statistics Canada also uses disaggregated data. This is data that is collected from multiple sources, then aggregated for reporting purposes, and then disaggregated again to learn about a particular issue. For example, to learn more about First Nations high school graduation rates, Statistics Canada would review information on high school graduation rates for all Canadians. It would then identify First Nations students in that group and explore their graduation rates alone. Statistics Canada is currently pursuing a data disaggregation strategy to "lead to detailed statistical information to highlight the experiences of specific population groups, such as women, Indigenous peoples, racialized populations and people living with disabilities" (Statistics Canada, 2021). Again, all this use of First Nations data and information is without any requirement to engage, consult, or seek approval of First Nations.

Under the *Access to Information Act*, the Crown reviews access to information requests to determine if they are "vexatious, made in bad faith, or otherwise an abuse of the right of access" (s. 6 and 6.1). The Crown may not deny access if the use intended will merely offend, embarrass, or otherwise disadvantage First Nations. This decision is left in the hands of the federal public service, further evidence of their unilateral approach. The Crown should not be permitted to make unilateral decisions about what may or may not harm First Nations in the release of their data and information. In the short term, the *Access to Information Act* could be amended to deny access to anonymized First Nations data and information to non-First Nations people and organizations that has not been approved by First Nations. In the longer term, however, the Crown must repatriate or at least divest itself of ownership of First Nations data and answer to First Nations for its use.

In addition, the Crown enriches itself and third parties by selling access to First Nations data. First, the Crown receives monetary gain every time a First Nations citizen, government, or organization files an access to information request. A fee of $5.00 must be paid when filing the request form (Treasury Board, 2014). Regardless of the small fee, the requirement of charging First Nations for access to their own information is yet another example of colonial tactics utilized by the Crown, which is further compounded as the Crown profits from each sale. This is particularly so, because First Nations can be required to submit access to information requests for everything from a list of their members to information on their fisheries. Second, the Crown sells First Nations data and information to third parties. This includes the sale of information about First Nation beneficiaries use of health services and goods including prescription drugs, medical transportation, dental care, and medical devices provided through the National Indian Health Branch. In 2001, Health Canada began releasing First Nations health data to a health consulting and analysis firm that in turn offered the data for sale to pharmaceutical companies for their own use. Health Canada felt justified because the data had been de-identified, and there would therefore be no privacy implications (FNIGC, 2014). In any case, Health Canada reasoned, the company would be entitled to the information under an access to information request, because it is information under the government's control.

Universities, colleges, and other research institutions also are granted access to First Nations data (*Privacy Act*, s.8(j)). This includes through the Research Data Centres noted above. Many academics and universities rely on the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (Tri-Council, 2018) to address the use of data in research. This policy statement does not fully address the First Nations principles of OCAP® and thus does not adequately address First Nations data sovereignty. Many would argue that access advances human knowledge and capacity by making data and information open and available (CANARIE/Research Data Canada, 2016). While this may be true, it also brings about profit, prestige, advancement,

and enrichment of non-Indigenous institutions and individuals at the expense of First Nations. There is inadequate consideration in Canada's information management regime of whether the compilation and release or sale of First Nations data may result in harm to First Nation communities or individuals.

The federal government is pursuing research data management strategies through many different policies and funding calls operated by a host of departments in an uncoordinated manner. First Nations data sovereignty requires a consistent, whole of government approach from the Crown, in a Nation-to-Nation relationship. The First Nation, not the federal government and not non-Indigenous institutions should be making decisions about who can have access to First Nations data and information. Anything less perpetuates the colonial regime.

First Nations have no mechanism(s) available to them to find out who has accessed 'personal information banks,' repositories of personal information held by the federal government (see section 10 of the *Privacy Act*). Personal Information Banks held by ISC, for example, include information on Treaty annuities and the Indian Registry. What information they contain and how they can be used are worth noting as examples of the vast breadth of personal information collected by the Crown on First Nations citizens and them alone. Treaty annuities personal information bank includes information on dates of birth or death, names, gender, contacts, band registration numbers, band membership status, marriages, family relationships, band name, special arrangements for child custody, missing individuals, or those with special needs. Consistent use of this includes by provincial governments to enforce provincial laws, by Health Canada to determine eligibility for Non-Insured Health Benefits, the Ontario Ministry of Natural Resources for reasons not provided. The Indian Register personal information bank includes names, contact information, dates of birth and death, photographs, adoption information, place of birth and other biographical information. Consistent uses are similar to those noted for the Treaty annuity personal information bank (ISC, 2022). Concerns about 'consistent use' have been identified earlier in this paper. These records are retained for 60 years by ISC and applications for registration are kept by ISC for 30 years and then transferred to Library and Archives Canada.

There is no accountability or reporting to First Nations about the creation of aggregate data through anonymizing personal data banks. There is no difference between personal data banks and aggregate data when personal databases can be easily anonymized and released without any restrictions under any privacy law. The Department of Justice notes that the personal information banks are not working well. They are cumbersome and not actually being used by individuals to search for their personal information, the original purpose for which they were established (DOJ, 2019d). Perhaps they are more likely used as a menu of First Nations data, available upon request to researchers and businesses alike. DOJ has suggested that federal public bodies need greater capacity to use and disclose personal information that has been de-identified (DOJ, 2020). Whether a revitalized *Privacy Act* allows for greater use and disclosure of de-identified personal information or not, First Nations data sovereignty must remain top of mind.

Data sharing

The Crown shares data on First Nations with many other governments, third parties, and increasingly, with the push for open data, the world. "Open Data is defined as structured data that is machine-readable, freely shared, used and built on without restrictions" (Government of Canada, 2019). Recall this is without the need for additional consent from individuals who submitted their information to the Crown, for example to Indigenous Services Canada for the purpose of the Indian Registry (s.8(2)(j)). Issues of access have been addressed elsewhere, so this section will focus on data linkage and open data.

One reason personal information is shared is to facilitate linking two different data sets. The development of the Longitudinal Indian Registry Dataset (LIRD) is an example of data linkage research currently conducted by the federal government. It links the personal information contained in the Indian Registry with personal information from tax files held by the Canadian Revenue Agency. By having temporary access to the personal information, researchers and statisticians can confirm the accuracy of computer matching systems. The final combined data set is then stripped of any personal information and multiple other researchers and statisticians can use the resulting data base without need of accessing the personal information behind the numbers, nor triggering limitations posed by the *Privacy Act*. Statistics Canada has conducted the LIRD linkage and proposes to conduct statistical analysis of it. First Nations, including in Ontario, BC, Manitoba, and Nova Scotia have also used data linkage of the Indian Registry and provincial health information to improve health services to their citizens. They first sought permission from the First Nations to link the data and continue to be guided by First Nations governments in their use of the linked data set. Data linkage is not inherently bad. The concern lies with who is creating the data sets and for what purpose. Data sharing and linkage has real value to First Nations, but they need to be central to the decision-making process to defend the OCAP® principles.

The advent of networked computers has enhanced the capacity to share data globally. The push for open data access, laudable in many ways, undermines First Nations data sovereignty if their information is shared without their consent.

> *Despite being the rights holders in relation to data about them or for them, Indigenous peoples across nation-states remain peripheral to the channels of power through which consequential decisions about Indigenous statistics are made. This marginalisation continues within open data discussions, [and] the open data community (Raine, 2019).*

Researchers and government officials digitize First Nations data and information uploading it to the global commons, often without regard for First Nations data sovereignty, the potential to damage First Nations intellectual property rights, or the implications of sharing First Nations languages and cultures (Raine, 2019). Canada's 2018-2020 National Action Plan on Open Government includes the following commitment.

> *The Government of Canada will engage directly with First Nations, Inuit and Métis rights holders and stakeholders to explore an approach to reconciliation and open government, in the spirit of building relationships of trust and mutual respect. This commitment has been purposely designed to allow for significant co-creation and co-implementation, encouraging First Nations, Inuit, and Métis rights holders and stakeholders to define their own approaches to engagement on open government issues (Treasury Board, 2018).*

This commitment needs to be applied across Canada's information management regime, which is deeply implicated in potential abuses via open data.

Control and possession

Canada has control and possession of large amounts of First Nations data. Data and information under the control of Canada is required to be preserved for future generations under the *Libraries and Archives Canada Act*. Section 12 stipulates that no government or ministerial record may be disposed of or destroyed without approval of the Chief Librarian and Archivist. This means all information in the Government's control must be passed to the Chief Librarian and Archivist and all of it may eventually be made public. There is no exception for First Nations data beyond those First Nations listed by name in the *Privacy Act* and *Access to Information Act*. The Crown demands reams of information from First Nations demonstrated by successive audits by the Auditors General. This includes personal information for various purposes, as well as administrative and financial data, traditional

knowledge for environmental assessments, health data through the First Nations Inuit Health Branch, and so on. This is all considered by First Nations to be their data and information, not the Crown's.

This raises many questions about how to distinguish between Canada's data and First Nations data that is in Canada's possession. Is Canada the owner of the data by virtue of its control and possession? Or is the Crown merely steward of First Nations data when in its control and possession? This goes to the heart of the issue of First Nations data sovereignty. "First Nations must be able to bring any data or information resources collected by them or about them into their jurisdiction, whether by possession within their territory or by exercising their jurisdiction through other means" (FNIGC, 2020). Some specific suggestions for addressing this issue are provided in the recommendations section below.

Access to information

As noted earlier, Canada's *Privacy Act* both secures personal information and makes it accessible under particular circumstances. Section 8(2)(k) of the *Privacy Act* permits access to personal information by "any Aboriginal government, association of Aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the Aboriginal Peoples of Canada." This provision in the *Privacy Act*, must be read in conjunction with the *Access to Information Act*, as it too contains provisions addressing access. DOJ has acknowledged the need of First Nations to access data for claims research and notes in its 2020 Discussion Paper that there is a need to explore "the disclosure of personal information for such purposes" (DOJ, 2020). First Nations experience can help inform this conversation.

In 2017, when the *Access to Information Act* was being amended, the National Claims Research Directors, a national body mandated to research and develop specific claims on behalf of First Nations, submitted commentary on the proposed legislation to the Standing Committee on Access to Information, Privacy and Ethics (National Claims Research Directors, 2017). The Directors noted the Crown, who is the defendant in specific claims cases, is in a conflict of interest. The Crown controls the access to this information and has a vested interest in denying access to avoid making redress. Any effort by the Crown to restrict access to information essential to proving the claim is a denial of justice. In their submission the Directors state,

> *There was a protocol on informal access requests which was put into place two decades ago – this was to serve as an alternative to formal ATI [access to information] requests, and explicitly intended to facilitate ease of access of materials required to document First Nations' claims, disputes and grievances. But over successive governments it was eroded to the point where it is currently dysfunctional, and badly in need of repair and a renewed commitment. In the meantime, we have been forced to rely more on the formal ATI route which, based on our day-to-day experience, is characterized by non-cooperation, non-disclosure and unreasonable delay. There is a culture of indifference, secrecy, and non-disclosure at INAC which has yet to be dismantled or fully addressed (National Claims Research Directors, 2017).*

They went on to challenge the adoption of proposed amendments to section 6 of the *Access to Information Act* that they feared would further restrict access. Fortunately, the proposed amendments were not adopted, but that has not completely addressed First Nations' concerns about access through the application of the *Access to Information Act* or the *Privacy Act*.

For example, Canada has at times rejected First Nations' requests for information unless it falls within the subsection 8(2)(k) exception or is inconsistent in their application of this section and section 8(2)(j). First Nations need access to personal information held by the federal government for a host of reasons beyond researching claims including

for administrative, health, and social well-being purposes. These uses are not clearly authorized under the *Privacy Act* and the Crown uses this as an excuse to frustrate First Nations access.

As both the Truth and Reconciliation Commission and the National Inquiry into Missing and Murdered Indigenous Women and Girls, learned, the federal government is at times reluctant to release information (The Star, 2012; CBC, 2018). Commissioner Murray Sinclair has called the lack of government cooperation "tragic because it means the information around the full and complete story of the residential school experiences… is not going to be told" (CBC, 2020). This undermines transparency and accountability, key principles of any information management regime. It is a matter of the honour of the Crown to be forthcoming in these situations.

Retention and disposal

Just as the interconnection of the *Privacy Act*, *Statistics Act*, and *Access to Information Act* hinders First Nations data sovereignty, so too does the interconnection with the *Libraries and Archives Canada Act*. The *Libraries and Archives Canada Act* facilitates the retention of Canada's documentary history and makes it available to the public. It and the *Privacy Act* operate allow virtually all First Nations personal information to be held in perpetuity by the Canadian government.

The *Privacy Act* provides for the adoption of regulations to guide the disposal of personal information (s.6(3)). To date, no such regulations have been issued. Instead, the Office of the Privacy Commissioner has issued guidelines. Government institutions also are required to abide by relevant Treasury Board policy instruments and the Communications Security Establishment Canada's standards (Office of the Privacy Commissioner, 2014). The general rule is that all personal information held by the federal government must be retained for "at least two years", to allow time for individuals to access their personal information and correct it if needs be (DOJ, 2019a). The *Library and Archives of Canada Act*, however, stipulates that no record within government control may be disposed of or destroyed. It must all go to the National Archives unless there is a Records Disposition Order (RDO) from the National Archivist. There are not many RDO's that permit the destruction of records. The result is that personal information held by the Crown is retained at the discretion of each government institution until it goes to the National Archives. In the case of ISC, personal information that is contained in the Personal Information Banks includes the Indian Registry, band elections, Treaty lands, and Treaty annuities. This information is "retained by the Department for 30 years after the last action and then transferred to Library and Archives Canada" (ISC, 2022). It is then at the discretion of the Librarian and Archivist to decide if and how to dispose of the information (s.9(1) *Libraries and Archives Canada Act*). It can be held in perpetuity if that is the decision. There is no right of appeal from decisions of the Chief Librarian and Archivist if they have exercised their discretion within the principles of administrative law.

Even though control of the data and information has shifted from the department to the Archives, the Crown may not make personal information publicly available until 110 years following the birth of the individual to whom the information relates. This applies to non-First Nations people as well, but as noted earlier, the amount and types of information available on First Nations' citizens is far beyond information collected on others. Recall that the ISC data is an extraordinary bank of personal information on First Nations' citizens which has no equivalent for non-Indigenous people in Canada. The disclosure of this information has the potential to cause harm to First Nations communities, families, and individuals.

Publication

> *[S]tatistics about Indigenous peoples often perpetuate a narrative of inequality, creating a dominant portrait of Indigenous peoples as defined by their statistically measured disparity, deprivation, disadvantage, dysfunction, and*

difference. Data infrastructures are designed based on cultural assumptions that can lead to the systematic misrepresentation of Indigenous peoples" (Raine, 2019).

The cumulative effect of Canada's information management regime strips First Nations of opportunities to tell their own story. The information regime robs First Nations people of the opportunities for research with First Nations, by First Nations, and as interpreted and published by First Nations. As noted above, First Nations at times are denied access to their information. This restricts their capacity to learn about themselves and govern in the best interests of First Nations' citizens. At other times, the information is used by the Crown or sold indiscriminately to third parties for research who may have absolutely no experience or knowledge of First Nations people other than through their own interpretation of the data. This leads to a steady stream of analysis often unfavourable to First Nations, like how likely First Nations people are to be murdered or commit murder (Statistics Canada, 2019c), die from suicide (Statistics Canada, 2019d), or live in poor housing conditions (Statistics Canada 2019e). Maggie Walter refers to these types of publications as the Five D's of data on Indigenous peoples: "disparity, deprivation, disadvantage, dysfunction and difference" (Walter, 2016). The research is usually pursued to further the interests of the researchers, not the interests of First Nations. Further, this research can lead to opportunities for non-Indigenous researchers to profit financially or in prestige from access to information that First Nations themselves are sometimes denied. It also leads to the perpetuation of stereotypes and racism. First Nations are the most studied peoples in Canada, yet there appears to be little interest or opportunity for First Nations to tell their own stories, through their own eyes and lived experience.

This concludes the review of Canada's information management regime. As described in this section, there are multiple interconnected challenges and frustrations for First Nations. This includes general problems of colonial governance, a preference for individualism over collective rights, denial of First Nations rights to self-government and self-determination, as well as specific problems with consent, over-collection, and profit by the Crown from the sale of First Nations information. The *Privacy Act*, *Statistics Act*, *Access to Information Act*, and *Libraries and Archives Canada Act* have especially damaging impacts on First Nations data sovereignty and self-determined data governance. Collectively they amount to an abuse of power and denial of First Nations constitutional rights. In this next section we turn to a review of possible solutions.

Possible Solutions

It is not the place of FNIGC, a technical organization, to offer or endorse specific amendments to legislation. That is rightly the place of each First Nation independently or collectively through their various governing bodies, for example Treaty organizations or the Assembly of First Nations. Canada has a legal duty to consult with First Nations when the Crown contemplates new or amended laws, policies, and programs (*Haida* v. *British Colombia*, 2001). Technical level discussions with FNIGC do not qualify as consultation, because FNIGC is not a First Nations rights holder. These consultations must be conducted directly with the First Nations. What FNIGC can offer are some suggestions for further consideration and discussion by First Nations in reaching their own conclusions on how to proceed. These suggestions are gathered here below. They reference the systemic and specific problems with the legislation discussed earlier.

First and foremost, Canada is encouraged to embrace its legal obligations and policy commitments to work with First Nations to decolonize its information management regime. Decolonizing the system would include:

1. Respecting section 35 constitutional rights, Supreme Court of Canada decisions, and commitments from successive Prime Ministers;
2. Respecting international commitments like Treaties and the *United Nations Declaration on the Rights of Indigenous Peoples*;
3. Respecting First Nations proper place in the federation – including embracing reconciliation, Nation-to-Nation relations, free, prior and informed consent, co-development, and recognition of alternative legal orders; and
4. Fully acknowledging and respecting First Nations rights to self-determination and self-government and according them the same respect as other governments.

Respecting First Nations as governments would require the Crown to embrace multilateralism to respect First Nations data sovereignty. A multilateral approach is based on a Nation-to-Nation relationship, where each government maintains sovereignty over its data. A multilateral system would replace the Crown's current unilateral approach, where the Crown perceives itself to be the owner of First Nations data under its control with full proprietary rights in the data including the right to sell it, destroy it, or make it public. First Nations data sovereignty is an essential element of First Nations self-determination and self-government. This includes respecting the First Nation principles of OCAP®, which include First Nations ownership of, control over, access to, and possession of their data and information.

A multilateral system would require a short-term and a long-term fix. In the short-term, federal departments require guidance by First Nation decision-makers respecting data under their control. Pan-First Nation selected, operated, and interconnected data oversight review boards independent of, but embedded in every government institution that handles First Nations data could provide this oversight. These First Nation review boards might hold full decision-making authority respecting access to and publication of First Nations data held by the government institution. Departments that regularly engage First Nations data and information including Indigenous Services Canada (ISC), Crown - Indigenous Relations and Northern Affairs Canada (CIRNAC), Statistics Canada, Environment Canada and Climate Change, Natural Resources Canada, Employment and Social Development Canada, and others, could support First Nations data sovereignty with such oversight.

First Nations decision-making bodies would review requests to access or share First Nations' data, determine if additional consent is required and how it will be obtained, decide on the level of access and the type of data or information that will be shared, the processes, protocols and methodology of sharing, the review and approval of publications based on First Nations data and information, and/or

take decisions about the disposal or archiving of data and information. These bodies could also assist Canada in addressing the Auditors General's concerns regarding First Nations data by working with the government institution to identify instances of over-collection and make better use of existing data.

Many First Nations are ill-equipped at present to manage sophisticated data governance systems. They do not necessarily have the hardware and software, like access to high-speed internet, stand-alone computer servers or secure cloud-based servers, or trained personnel to be their own data stewards. An alternative or temporary solution is required, one that would not require a physical transfer of the data and information from the Crown to First Nations. In this instance, the Crown could act more like a bank for First Nations data. Only the 'account holders' – the First Nations – would have access to the data and only they would determine what happens to the data and information stored in the 'bank.' Canada might want to borrow this data and information from time to time, but that would be subject to approval by the First Nations affected. The data would not be in the First Nations physical possession, but it would be in their legal possession. Simply by shifting its perspective about its relationship to First Nations data, the Crown could move from owner to steward of the data, and thus respect OCAP®.

This is a simple solution that may not require amendments to legislation, merely internal policies. Section 2 of the *Libraries and Archives Canada Act*, for example, stipulates that documentary information under Canada's control must be turned over to Libraries and Archives Canada. If Canada were only steward of the data, it would not be in control of the data, thus the application of section 2 would be avoided. The Crown would enter into agreements with First Nations to serve as data steward under negotiated arrangements. Many First Nations in Ontario, Nova Scotia, and BC are already working with the federal government, provincial governments and/or third parties that are filling the need for data stewardship beyond the current capacity of First Nations. This includes the tripartite arrangement between the federal government, BC provincial health authority, and the BC First Nations Health Council (FNHA, 2011), the agreement between the Chiefs of Ontario and ICES (Institute for Clinical Evaluative Sciences) (Pyper, 2018), and the Tui'kn Partnership between five Mi'kmaq communities, Nova Scotia Department of Health and Wellness, and Health Canada (Tui'kn Partnership, n.d.a). These agreements establish stewardship of First Nations health data under First Nations' control. This might be a short-term fix for some First Nations. Others might wish to pursue longer-term agreements for this arrangement.

Over the longer-term, the First Nations Data Governance Strategy foresees Nation-based data sovereignty. This requires moving the data and the decision-making about the data to First Nations ownership, control, access, and possession. A multilateral system requires fully functioning and effective First Nations data management and oversight. For this multilateral system to advance, the Crown must reconsider its position *viz-a-viz* First Nations data. Instead of owner of the data, the Crown needs to consider itself in a custodial position operating at the direction of First Nations (Nickerson, 2017). The Crown would be obliged to seek direction every time a third party or the Crown itself sought access to the information. The Crown would no longer be free to sell First Nations data, charge First Nations for access to their data, nor create barriers to First Nations access to their data and information. New protocols and processes would be required for the retention and disposal of First Nations data held by the Crown. First Nations data would not be automatically open and available under the Treasury Board Open Data Guidelines. A simple shift in perspective from owner to custodian would have system-wide repercussions in support of First Nations data sovereignty.

As a side note, there would be a need to strike a joint federal-First Nation committee to dialogue on separation of First Nations data from that

legitimately owned by the Crown and to support data repatriation. There are times that Canada has legitimate needs and obligations to protect and provide access to data, which may, from time to time include First Nations' data. This needs to be acknowledged, but Canada and First Nations need to work together to determine how those needs and obligations will respect First Nations data sovereignty. Where data and information are deemed to be the Crowns, the Crown must be cautious to allow free, liberal, and timely access to First Nations data in researching claims against the Crown.

Cooperative engagement between the Crown and First Nations can improve awareness and understanding about Canada's information management regime and its impact on First Nations. There are opportunities to learn from each other. The Privacy Commissioner, the Information Commissioner, and the Chief Librarian and Archivist represent functions that First Nations may want to reflect upon and possibly adopt within their own data governance and management systems. Likewise, Canada has much to learn from First Nations, including how to engage a holistic approach to governance.

The information management regime needs a system-wide overhaul and a commitment to a whole of government approach in its implementation. Addressing the *Privacy Act* in isolation from the other parts of Canada's information management regime may help to address some irritants but would otherwise leave Canada's colonialist domination over First Nations' data and information intact. To use a car analogy, a new paint job on a car with a broken engine block is not going to make the car run any better. Tinkering with Canada's information management regime to add a definition here (DOJ, 2019c) or expand the power of the Office of the Privacy Commissioner to engage in public education there (DOJ, 2019c) is not going to fix the fundamental colonialism found in this legislation. We need to remove Crown unilateralism and replace it with multilateral cooperation and recognition of clear boundaries between Crown and First Nations' data sovereignty. Why fix a car that never took First Nations anywhere? Let us build a new car together, one that runs on the sustainable fuel of multilateral cooperation.

Conclusion

This discussion paper has clearly identified a conflict between Canada's information management regime and First Nations rights. The existing regime is fundamentally incompatible with First Nations' data sovereignty. The entirety of the information management regime, not just the *Privacy Act*, fails to respect the principles of OCAP® and needs a system-wide overhaul.

At a macro level, the Crown needs to recognize and accommodate First Nations' collective rights to privacy. First Nations' privacy is greater than the individual privacy rights of its citizens. The Crown needs to recognize all First Nations as legitimate governments and treat their data with the same respect as data received from other nations and governments. Even municipalities have greater rights to share information in confidence than First Nations under federal laws. The Crown must halt its current unilateral approach to decision making about First Nations' data and information and embrace a multilateral approach that puts First Nations in the driver's seat respecting their own data and information. Engaging First Nations as decision makers facilitates their data sovereignty. It is the antidote to colonialism.

There are a host of specific problems with the various laws and the ways they interact. This includes ill-defined terms, like 'necessity', 'public interest,' and 'consistent use' that do little to prevent misuse of First Nations' data and information. The fact that the Crown is enriched through the sale of First Nations' data and information to third parties is a serious breach of First Nation data sovereignty. Often it is these same third parties, along with the Crown, who perpetuate negative stereotypes of First Nations through their ill-informed interpretation of the data and information. At the same time, they enrich themselves in prestige, promotions, and academic achievement. Likewise, the Crown has at times denied or attempted to frustrate First Nations' access to their own information. This is especially problematic when First Nations are seeking access to information they need to improve the lives of their citizens or when they are researching claims against the Crown. The over-collection of information on First Nations, decried many times by Canada's Auditors General, lends itself to greater opportunities for abuse and breach of First Nations' privacy. In addition, the Crown relies on impaired provisions of consent to get access to and make wide use of First Nations data. Many other problems have been identified here, all of which demand attention.

Multiple suggestions are included in this paper for addressing the problems highlighted. To summarize this includes:

1. System wide overhaul
2. Address the colonialism inherent in the system
   (a) Respect Canadian law (*Royal Proclamation, 1763*, *Constitution Act, 1982*, Supreme Court of Canada decisions (Sparrow, Haida, Pamajewon), commitments from the Prime Ministers;
   (b) Respect international commitments (UNDRIP, Treaties);
   (c) Do this in a fashion that respects First Nations role in the federation – reconciliation, Nation-to-Nation, free, prior, and informed consent, co-development, and recognition of alternative legal orders; and
   (d) Fully acknowledge and respect First Nations rights to self-determination and self-government and accord them the same respect as other governments
3. Embrace multilateralism
   (a) Establish and fund First Nation selected and operated First Nation data oversight review boards within every government institution with full decision-making authority respecting access to and publication of data and

support their coordination to ensure consistency – Short-term fix

(b) Cease the sale of First Nations data in any form, and exempt First Nations from access to information fees

(c) Cease making unreasonable demands on First Nations for perpetual free license for use of their intellectual property.

4. Change perspective on the Crown's relationship to the First Nations data it holds

(a) Presume a position of steward instead of owner of First Nations data held by the Crown – short-term fix for some, longer for others

(b) Enter into agreements with First Nations for Crown to serve as data steward if that is the desire of the First Nation;

(c) Fund the creation of First Nation-based data oversight review boards to provide direction to Canada in its role as data steward (these are not the same as the ones established within departments) as a long-term fix

(d) Inform First Nation review boards when access to Crown held First Nation data is sought by third parties so that First Nation data oversight boards can review requests and make decisions about allowing the access;

(e) Work with Libraries and Archives Canada and First Nations to develop new definitions, protocols, and processes for the retention and disposal of First Nations data, public access to First Nations data, and repatriation of the data

(f) Strike a joint federal – First Nation working group to dialogue on separation of First Nations data from that legitimately owned by the Crown

5. Fully address the Auditors General's concerns about the over-collection of First Nations data; and

6. Have due regard to the Crown's position as potential adversary in First Nations claims against the Crown and facilitate free, liberal, and timely access to data for claims research

The tentacles of colonialism reach deep and wide, including into the esoteric world of information management. It is the identification and severing of these tentacles that is the work ahead, not only for First Nations, but in and with the fully engaged cooperation of the Crown.

Resources

Legislation and international instruments

Access to Information Act (R.S.C., 1985, c.A-1)

British Columbia Tripartite Framework Agreement on First Nation Health Governance, 2011, https://www.fnha.ca/Documents/framework-accord-cadre.pdf

Canadian Human Rights Act (S.C. 1976-77, c. 33, s. 1) (original citation)

Charter of the United Nations, 1945, https://www.un.org/en/sections/un-charter/un-charter-full-text/

Declaration on the Rights of Indigenous Peoples Act [SBC 2019] CHAPTER 44, https://www.bclaws.ca/civix/document/id/complete/statreg/19044

Income Tax Act (R.S.C., 1985, c.1 (5th Supp.))

Library and Archives of Canada Act (S.C. 2004, c. 11)

Memorandum of Understanding between the Department of Citizenship and Immigration of Canada and the Canada Border Services Agency and the Department of Immigration and Border Protection of the Commonwealth of Australia Regarding the Exchange of Information (2016), https://www.canada.ca/en/immigration-refugees-citizenship/corporate/mandate/policies-operational-instructions-agreements/agreements/um-arrangement-canada-border-services-agency-new-zealand-ministry-business-innovation.html

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

Privacy Regulations (SOR/83-508)

Quebec Charter of Human Rights and Freedoms, Chapter C-12, https://www.legisquebec.gouv.qc.ca/en/document/cs/c-12

Statistics Act, (R.S.C., 1985, c. S-19)

Tsawwassen First Nation, 2009, *Freedom of Information and Protection of Privacy Act*, http://tsawwassenfirstnation.com/wp-content/uploads/2019/07/Freedom_of_Information_and_Protection_of_Privacy_Act_WEB_17_Jul_2017.pdf

United Nations Declaration on the Rights of Indigenous Peoples, : resolution / adopted by the General Assembly, 2 October 2007, A/RES/61/295, https://www.un.org/development/desa/indigenouspeoples/declaration-on-the-rights-of-indigenous-peoples.html

Case citations

Behn v. *Moulton Contracting Ltd.* [2013] 2 S.C.R. 227

Bernard v. *Canada* (Attorney General) [2014] 1 S.C.R. 227

Calder et al. v. *Attorney-General of British Columbia* [1973] SCR 313

Delgamuukw v. *British Colombia* [1997] 3 S.C.R. 1010

Haida Nation v. British Columbia (Minister of Forests) [2004] 3 S.C.R. 511

R. v. *Gladstone* [1996] 2 S.C.R. 723

R. v. *Pamajewon* [1996] 2 S.C.R. 821

R. v. *Van der Peet* [1996] 2 S.C.R. 507

Tsilhqot'in Nation v. *British Columbia* [2014] 2 S.C.R. 257

Tsilhqot'in Nation v. *British Columbia*, 2007 BCSC 1700

Government sources

Bennett, Honourable Carolyn, 2016, *Canada Becomes a Full Supporter of the United Nations Declaration on the Rights of Indigenous Peoples*, https://www.canada.ca/en/indigenous-northern-affairs/news/2016/05/canada-becomes-a-full-supporter-of-the-united-nations-declaration-on-the-rights-of-indigenous-peoples.html

Department of Justice (DOJ), 2020, *Respect, Accountability, Adaptability: A discussion paper on the modernization of the Privacy Act,* https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/raa-rar.html#s1

DOJ, 2019a, *Privacy Act Modernization: A Discussion Paper - Privacy Principles and Modernized Rules for a Digital Age*, https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/dp-1.pdf

DOJ, 2019b, *Privacy Act Modernization: A Discussion Paper - Transparency and accountability: demonstrating the commitment and respect necessary to facilitate trust*, https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_2.html

DOJ, 2019c, *Privacy Act Modernization: A Discussion Paper - Greater certainty for Canadians and government: delineating the contours of the Privacy Act and defining important concepts*, https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_3.html

DOJ, 2019d, *Privacy Act Modernization: A Discussion Paper - A modern and effective compliance framework with enhanced enforcement mechanisms*, https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_4.html

DOJ, 2019e, *Privacy Act Modernization: A Discussion Paper - Modernizing the Privacy Act's relationship with Canada's [sic] Indigenous peoples*, https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_5.html

Government of Canada, 2019, *Open Data 101*, https://open.canada.ca/en/open-data-principles

Immigration, Refugees, and Citizenship Canada (2018) *Agreements with other departments and governments*, https://www.canada.ca/en/immigration-refugees-citizenship/corporate/mandate/policies-operational-instructions-agreements/agreements.html

Indigenous Services Canada, 2019, 2020-2021 *Comprehensive Funding Agreement (with 10-year grant)* 2020-2021, https://www.sac-isc.gc.ca/eng/1575757514392/1575757541459

Indigenous Services Canada, 2022, *Info Source: Sources of Federal Government and Employee Information for Indigenous Services Canada*, https://www.sac-isc.gc.ca/eng/1639748667069/1639748703555

Indigenous Services Canada, 2020, *Application For Registration On The Indian Register And For The Secure Certificate Of Indian Status*, https://www.sac-isc.gc.ca/DAM/DAM-ISC-SAC/DAM-INSTS/STAGING/texte-text/br_frms_ir_83-168_print_1525977093102_eng.pdf

Libraries and Archives Canada, 2020, *Indigenous Documentary Heritage Initiatives,* https://www.bac-lac.gc.ca/eng/discover/aboriginal-heritage/initiatives/Pages/default.aspx

Libraries and Archives Canada, 2019, LAC Committees and Advisory Groups, https://www.bac-lac.gc.ca/eng/transparency/briefing/2019-transition-material/Pages/corp-sec-committees-advisory-groups.aspx

Minister of Justice, 2017, *Government Response To The Fourth Report Of The Standing Committee On Access To Information, Privacy And Ethics*, https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-4/response-8512-421-135

National Inquiry into Missing and Murdered Indigenous Women and Girls (2019) *The Final Report of the National Inquiry into Missing and Murdered Indigenous Women and Girls,* https://www.mmiwg-ffada.ca/final-report/

Office of the Auditor General, 2002, *Stream Lining First Nations Reporting to Federal Organizations*, http://publications.gc.ca/collections/collection_2012/bvg-oag/FA1-2002-2-9-eng.pdf

Office of the Auditor General, 2006, *2006 Status Report*: "Chapter 5 Management of First Nations Programs", https://www.oag-bvg.gc.ca/internet/docs/20060505ce.pdf

Office of the Auditor General, 2011, *June 2011 Status Report* "Chapter 4: Programs for First Nations on Reserve", https://publications.gc.ca/collections/collection_2011/bvg-oag/FA1-10-2011-4-eng.pdf

Office of the Auditor General, 2018, *2018 Spring Reports of the Auditor General of Canada to the Parliament of Canada*, "Report 5—Socio-economic Gaps on First Nations Reserves—Indigenous Services Canada", https://www.oag-bvg.gc.ca/internet/English/parl_oag_201805_05_e_43037.html

Office of the Privacy Commissioner (OPC), 2016, *The federal government and your personal information*, https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rights/the-federal-government-and-your-personal-information/

Office of the Privacy Commissioner (OPC), 2014, *Personal Information Retention and Disposal: Principles and Best Practices*, https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/safeguarding-personal-information/gd_rd_201406/

Organization of Economic and Cooperation and Development (OECD), 1980, *OECD Privacy Principles,* http://oecdprivacy.org/

Organization of Economic and Cooperation and Development (OECD), 2013, *The OECD Privacy Framework*, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Parliamentary Standing Committee on Access to Information, Privacy and Ethics, 2016a, https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html

Parliamentary Standing Committee on Access to Information, Privacy and Ethics, 2016b), https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-4/

Privy Council Office, 2020, *Speech from the Throne*, https://www.canada.ca/en/privy-council/campaigns/speech-throne/2020/speech-from-the-throne.html

Royal Commission on Aboriginal Peoples (1996) *Report of the Royal Commission on Aboriginal Peoples,* https://www.bac-lac.gc.ca/eng/discover/aboriginal-heritage/royal-commission-aboriginal-peoples/Pages/final-report.aspx

Statistics Canada, 2022, Canadian Statistics Advisory Council, https://www.statcan.gc.ca/en/about/relevant/CSAC

Statistics Canada, 2021, *Disaggregated Data Action Plan: Why it matters to you*, https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2021092-eng.htm

Statistics Canada, 2020a, Population estimates, quarterly, https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1710000901

Statistics Canada, 2020b, *Research Data Centres*, https://www.statcan.gc.ca/eng/microdata/data-centres

Statistics Canada, 2019a, *Total population by Aboriginal identity and Registered or Treaty Indian status*, Canada, 2016, https://www12.statcan.gc.ca/census-recensement/2016/as-sa/fogs-spg/Facts-CAN-eng.cfm?Lang=Eng&GK=CAN&GC=01&TOPIC=9

Statistics Canada, 2019b, *Guide to the Census of Population, 2016, Chapter 11 – Dissemination*, https://www12.statcan.gc.ca/census-recensement/2016/ref/98-304/chap11-eng.cfm

Statistics Canada, 2019c, *Number of homicide victims and persons accused of homicide, by Aboriginal identity, age group and sex,* https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510006001

Statistics Canada, 2019d, *Suicide among First Nations people, Métis and Inuit (2011-2016): Findings from the 2011 Canadian Census Health and Environment Cohort (CanCHEC),* https://www150.statcan.gc.ca/n1/pub/99-011-x/99-011-x2019001-eng.htm

Statistics Canada, 2019e, *Results from the 2016 Census: Housing, income and residential dissimilarity among Indigenous people in Canadian cities,* https://www150.statcan.gc.ca/n1/pub/75-006-x/2019001/article/00018-eng.htm

Treasury Board of Canada Secretariat (TBS), 2010, *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*

Treasury Board, 2014, *Access to Information Request Form*, https://www.tbs-sct.gc.ca/tbsf-fsct/350-57-nf-eng.pdf

Treasury Board, 2018, *Canada's 2018-2020 National Action Plan on Open Government*, https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government#toc12

Trudeau, Prime Minister Justin (2015), *Statement by Prime Minister on release of the Final Report of the Truth and Reconciliation Commission*, https://pm.gc.ca/en/news/statements/2015/12/15/statement-prime-minister-release-final-report-truth-and-reconciliation

Trudeau, Prime Minister Justin (2015), *Statement by Prime Minister on the International Day of the World's Indigenous Peoples*, https://pm.gc.ca/en/news/statements/2020/08/09/statement-prime-minister-international-day-worlds-indigenous-peoples

Truth and Reconciliation Commission of Canada. (2015). *The Final Report of the Truth and Reconciliation Commission of Canada,* http://nctr.ca/reports.php;

Other sources

Banks, S., & Hébert, M. (2004). Legislative summary: Bill C - 8: The Library and Archives of Canada Act, https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/37-3/c8-e.pdf

Borrows, John, 2019, *Law's Indigenous Ethics*, University of Toronto Press

CANARIE/Research Data Canada, 2016, *Creating Canada's Action Plan on Open Government 2016–18*, https://open.canada.ca/en/idea/open-data-innovation

CBC, 2020, *Ottawa's lack of co-operation over residential school claim records 'tragic,' says Murray Sinclair*, CBC, June, 2, 2020, https://www.cbc.ca/news/indigenous/murray-sinclair-iap-records-1.5593634

CBC, 2018, *Missing and murdered Indigenous women's inquiry wages court fight for RCMP files*, CBC, April 15, 2018, https://www.cbc.ca/news/politics/mmiwg-rcmp-court-files-1.5098052

CIRA, 2018, *Data sovereignty: What you need to know and why you should care,* https://www.cira.ca/blog/state-internet/data-sovereignty-what-you-need-know-and-why-you-should-care

Clarke, Roger, 1997 "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997, http://www.rogerclarke.com/DV/Intro.html

Cohen, Julie E., 2012, "What Privacy Is For", 126 HARV. L. REV, 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2175406

Dijkstra, Edsger W, 1982, "On the role of scientific thought". Selected writings on Computing: A Personal Perspective. New York, NY, USA: Springer-Verlag. pp. 60–66. ISBN 0-387-90652-5.

Fanon, Franz, 1963, *The Wretched of the Earth*, Grove Atlantic Inc.

First Nations Health and Social Secretariat of Manitoba (FNHSSM), n.d., Health Information Research Governance Committee (HIRGC), https://www.fnhssm.com/hirgc

First Nation Health Authority, 2011, *British Columbia Tripartite Framework Agreement on First Nation Health Governance*, https://www.fnha.ca/Documents/framework-accord-cadre.pdf

FNIGC, n.d.a., *The First Nations Principles of OCAP®*, https://fnigc.ca/ocap-training/

FNIGC, 2014, Ownership, Control, Access and Possession (OCAP™): The Path to First Nations Information Governance, https://achh.ca/wp-content/uploads/2018/07/OCAP_FNIGC.pdf

FNIGC, 2020, *A First Nations Data Governance Strategy*, https://fnigc.ca/wp-content/uploads/2020/09/FNIGC_FNDGS_report_EN_FINAL.pdf

FNIGC, n.d.b. *About FNIGC*, https://fnigc.ca/about-fnigc/

Forget, Chloe (revised 2019) *Legislative Summary of Bill C-58 to Amend the Access to Information Act*, Library of the Canadian Parliament

Friedewald, Michael & Finn, Rachel & Wright, David. (2013). Seven Types of Privacy. 10.1007/978-94-.

Gee, Kimberley, 2019, *Introduction to Indigenous Canadian Conceptions Of Privacy: A Legal Primer*, https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2019/Runner-up-of-2019-Privacy-and-Access-Law-Student-E

Chief Stanley Grier First Nations Data Governance Strategy Summit February 26, 2019

Goodman, A., Morgan, R., Kuehlke, R., Kastor, S., Fleming, K., Boyd, J., Aboriginal Harm Reduction Society, W. (2018). "We've Been Researched to Death": Exploring the Research Experiences of Urban Indigenous Peoples in Vancouver, Canada. The International Indigenous Policy Journal, 9(2).

Hummel, Patrik; Braun, Matthias; Augsberg, Steffen; Dabrock, Peter (2018), *Sovereignty and Data Sharing* ITU Journal: ICT Discoveries, Special Issue No. 2, 23 Nov. 2018, https://www.itu.int/en/journal/002/Documents/ITU2018-11.pdf

INSPIRE Architecture and Standards Working Group, 2002, *INSPIRE Architecture and Standards Position Paper*, JRC-Institute for Environment and Sustainability, Ispra, https://inspire.ec.europa.eu/reports/position_papers/inspire_ast_pp_v4_2_en.pdf

Joint Advisory Committee on Fiscal Relations, 2019, *Honouring our Ancestors by Trailblazing a Path to the Future*, Ottawa, https://www.afn.ca/wp-content/uploads/2019/11/Interim-Report-of-the-Joint-Advisory-Committee-on-Fiscal-Relations-Jun...4.pdf

Kukutai, Tahu, Taylor, John (eds.), 2016, *Indigenous Data Sovereignty Toward an Agenda*, ANU Press, https://press-files.anu.edu.au/downloads/press/n2140/pdf/book.pdf

Mamalilikulla First Nation, n.d. *Mamalilikulla Privacy Policy,* https://mamalilikulla.ca/privacy-policy/

Mi'kmaw Ethics Watch, undated, Mi'kmaw Research Principles and Protocols, https://www.cbu.ca/wp-content/uploads/2019/08/MEW-Principles-and-Protocols.pdf

National Claims Research Directors, 2017, *Impaired Access Submission To The Standing Committee On Access To Information, Privacy And Ethics Regarding Bill C-58*, https://d3n8a8pro7vhmx.cloudfront.net/ubcic/pages/3558/attachments/original/1508159521/2017-10-16_NCRDSubmissionBillC-58FINAL.pdf?1508159521

Nickerson, Marcia, 2017, First Nations' Data Governance: Measuring the Nation-to-Nation Relationship, BCFNDGI, https://www.bcfndgi.com/

Open Geospatial Consortium, 2015, *OGC® WPS 2.0.2 Interface Standard Corrigendum 2*, http://docs.opengeospatial.org/is/14-065/14-065.html

Pyper, Evelyn; Henry, David; Yates, Erika A.; Mecredy, Graham; Ratnasingham, Sujitha; Slegers, Brian; and Walker, Jennifer D., (2018) "Walking the Path Together: Indigenous Health Data at ICES", Healthcare Quarterly 20(4) January 2018, https://www.longwoods.com/content/25431/walking-the-path-together-indigenous-health-data-at-ices

Rainie, S., Kukutai, T., Walter, M., Figueroa-Rodriguez, O., Walker, J., & Axelsson, P. , 2019, "Issues in Open Data - Indigenous Data Sovereignty", in T. Davies, S. Walker, M. Rubinstein, & F. Perini (Eds.), *The State of Open Data: Histories and Horizons*. Cape Town and Ottawa: African Minds and International Development Research Centre.

Rocher, Luc; Hendrickx, Julien M.; de Montjoye, Yves-Alexandre, 2019, "Estimating the success of re-identifications in incomplete datasets using generative models", in Nature Communications, https://doi.org/10.1038/s41467-019-10933-3

The Star, 2012, *Truth commission goes to court to get government documents*, The Star, December 3, 2012, https://www.thestar.com/news/canada/2012/12/03/truth_commission_goes_to_court_to_get_government_documents.html

Tsawwassen First Nations, 2019, *Tsawwassen Records and Information Management Policy,* http://tsawwassenfirstnation.com/wp-content/uploads/2019/07/Records_and_Information_Management_Policy_2011_09_28.pdf

Tui'kn Partnership, n.d.a, *Strength in Numbers Project*, http://www.tuikn.ca/current-initiatives/news-story-title/

Tui'kn Partnership, n.d.b, *About Tui'kn*, http://www.tuikn.ca/about-tuikn/

United Nations, n.d., *Big Data for Sustainable Development*, https://www.un.org/en/global-issues/big-data-for-sustainable-development

Vis-Dunbar, Megan; Williams, James; Jahnke, Jens H. Weber, 2011, *Indigenous and Community-based Notions of Privacy*, UVic/IPIRG.

Walter, Maggie. (2016). Data politics and Indigenous representation in Australian statistics. 10.22459/CAEPR38.11.2016.05.

Williams, James; Vis-Dunbar, Megan; Jahnke, Jens H. Weber, 2011, *Reconciling Individualistic and Communal Notions of Privacy*, UVic/IPIRG, https://www.researchgate.net/publication/310482010_Reconciling_Individualistic_and_Communal_Notions_of_Privacy

Wilson, Peigi, 2009, *Interconnections: The Symbiosis of Human Rights and Environmental Protection, An Argument for First Nation Environmental Governance*, LLM thesis, University of Ottawa.