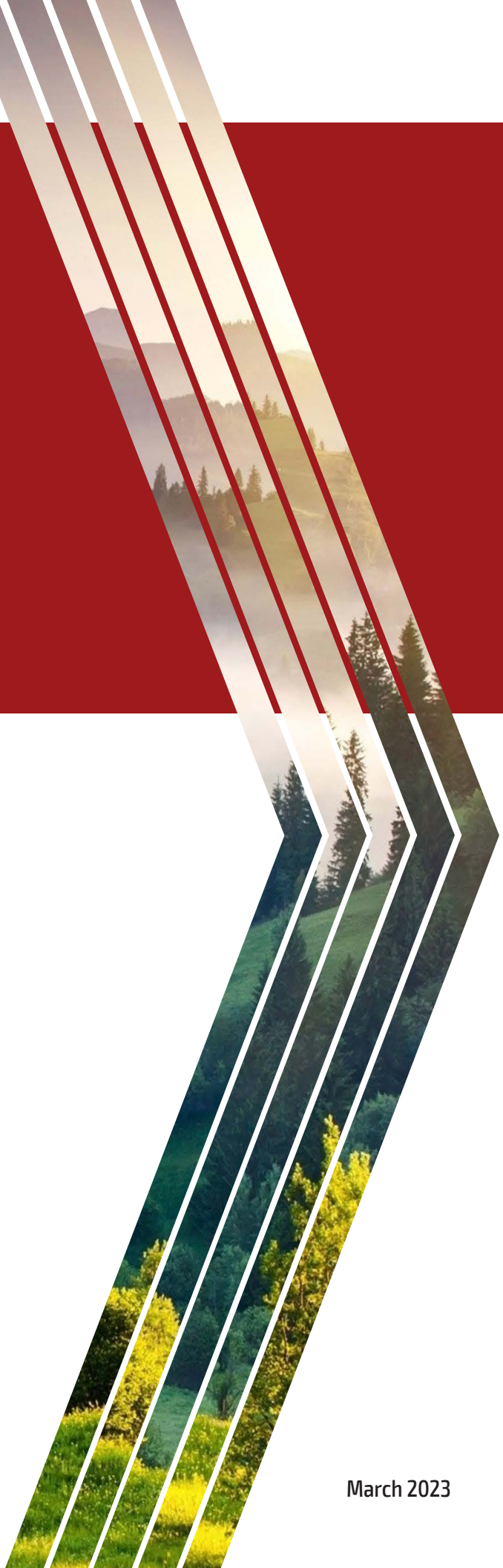
PIPEDA AND FIRST NATIONS: APPLICATION AND REFORM



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

March 2023

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: 978-1-988433-19-6

Our Work

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 distinct world views. FNIGC is strictly technical, apolitical, is not a rights-holding organization, and does not speak directly for First Nations. Mandated by the Assembly of First Nations' Chiefs-in-Assembly (AFN Resolution #48, December 2009), FNIGC's Mission is to assert data sovereignty and support the development of information governance and management at the community level through regional and national partnerships. 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.

FNIGC acknowledges with thanks the contributions to this paper by Professor Lisa M. Austin, University of Toronto Faculty of Law, Erica Berry, JD student, University of Toronto Faculty of Law, and David Baldridge, JD student, University of Toronto Faculty of Law.

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

This paper is not legal advice and should not be relied upon as such.

Contents

INTRODUCTION

This FNIGC Issue Paper explores the application of the *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c.5) (*PIPEDA*) to First Nations businesses, governments, and organizations, outlines some comparisons with equivalent provincial private sector privacy legislation, and considers options for PIPEDA's reform. This analysis of PIPEDA will include consideration of First Nations data sovereignty and the First Nations Principles of OCAP® in the context of personal information privacy in the private sector and for First Nations governments, as well as emerging issues in personal information privacy.

Chapter One provides an overview of PIPEDA and analogous provincial private sector laws. It outlines the basic obligations of such legislation, points to several important guidance documents, and discusses several decisions pertaining to Band Councils. It also outlines the changes proposed by the recently introduced Bill C-27, which creates the *Consumer Privacy Protection Act* (CPPA) to replace PIPEDA.

Chapter Two provides an overview of First Nations data sovereignty, the OCAP® principles, and the relevance of *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP) to data sovereignty claims. It then uses this overview to provide a critique and potential roadmap for Canadian private sector privacy law reform from the perspective of First Nations data sovereignty.

CHAPTER ONE: OVERVIEW OF PIPEDA AND PROVINCIAL PRIVACY LEGISLATION

OVERVIEW OF PIPEDA

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) (S.C. 2000, c.5) is Canada's federal private-sector privacy law. It sets out the ground rules for how businesses must handle the personal information that they collect, use or disclose in the course of commercial activities as well as how federal works, undertakings and businesses must handle personal employee information. Personal information is defined in the legislation to mean "information about an identifiable individual" (PIPEDA, s.2(1)).

The general requirements of PIPEDA are the 10 fair information principles set out in Schedule 1 (Office of the Privacy Commissioner of Canada, 2019a):

1. Accountability: this requires organizations to designate someone who is accountable for compliance.

2. Identifying Purposes: this requires organizations to identify up front the purposes for which personal information is being collected.

3. Consent: the knowledge and consent of the individual data subject is generally required (subject to exceptions enumerated in the legislation).

4. Limiting Collection: this requires that the personal information collected is limited to what is necessary for the identified purposes.

5. Limiting Use, Disclosure and Retention: personal information cannot be used for new purposes unless there is consent or the law requires this. It can only be retained as long as is necessary to fulfill the purpose of its collection.

6. Accuracy: this requires that personal information is accurate, complete, and up to date.

7. Safeguards: personal information is required to be protected by appropriate security safeguards.

8. Openness: organizations must provide information about their policies and practices.

9. Individual Access: organizations must provide individuals with access to their personal information upon request and amend it if inaccurate.

10. Challenging Compliance: individuals should be able to challenge compliance with these principles.

A central feature of PIPEDA is that an individual's informed consent is required unless an organization's collection, use or disclosure falls within one of the specifically enumerated exceptions (PIPEDA ss. 7(1)-(4)). However, informed consent to the collection of personal information is not sufficient to make the collection compliant with PIPEDA. The collection must also be limited to what is necessary for the purposes (PIPEDA, Schedule 1, Principle 4).

In addition, PIPEDA mandates that personal information may be collected, used, or disclosed "only for purposes that a reasonable person would consider are appropriate in the circumstances" (PIPEDA s. 5.3). Once collected, the personal information can only be used or disclosed in accordance with the consented-to purposes (subject to specifically enumerated exceptions and the "appropriate" requirement noted above). Further, the information must be accurate, kept securely, and only retained for as long as necessary. In the event of a data breach, PIPEDA outlines the steps that must be taken with respect to notification (PIPEDA Division 1.1). This includes reporting to the Office of the Privacy Commissioner of Canada (OPC) as soon as feasible of any breach of security if the breach could cause serious harm to an individual, and informing the individual of the breach (PIPEDA, Division 1.1.)

Complaints can be made by individuals or identified by the OPC (OPC, 2017a). Once a complaint is registered the OPC first must ensure that the issue in question falls within the scope of PIPEDA. The procedures and processes adopted by the OPC then require the Intake Unit to review the complaint and encourage complainants to resolve the issue with the organization directly (OPC, 2017a). If this is not possible, the OPC then starts to investigate the complaint and determine if it can be resolved through early resolution, or whether it should move onto formal investigation. Complaints that are candidates for early resolution will be passed onto the Early Resolution Officer. They are often those that can be resolved through mediation. If early resolution is not an option, the complaint will move onto a formal investigation, during which time the Commissioner will analyze the facts of the case and consult directly with the organization in question. Also, note that the Commissioner has broad powers to assist in resolving disputes including among others, summon witnesses and compel the provision of evidence, administer oaths, and enter premises (PIPEDA, s.12.1).

Once a formal investigation is complete, the Privacy Commissioner assesses the report, and determines whether recommendations should be made to the organization. If the OPC finds there was a contravention of PIPEDA, the Privacy Commissioner will advise the organization on how to remedy it. A final report will then be sent to the organization, which "outlines the basis of the complainant, the relevant findings of fact, the analysis, and the response of the organization to any recommendations made in the preliminary report" (OPC, 2015). The organization is advised to implement the recommendations made by the OPC, and the OPC can ask the organization to keep them updated. Finally, either the complainant or the OPC can apply to have the matter heard at the Federal Court. The Federal Court has the power to order the organization to correct its practices or award damages to the complainant (OPC, 2015).

The OPC has many guidance documents that offer helpful advice regarding how to comply with PIPEDA (e.g., OPC, 2008, 2017a, 2017b, 2019a, 2020). In what follows we will provide further details of aspects of the legislation that may be particularly helpful to First Nations.

APPLICATION OF PIPEDA

PIPEDA is federal legislation and so only applies to organizations and activities that fall within federal jurisdiction. To fall within federal jurisdiction, the First Nation entity is either engaged in commercial activities or holds employee information as a federal work, undertaking, or business (FWUB).

Personal information that an organization "collects, uses or discloses in the course of commercial activities" is regulated as part of the federal government's trade and commerce power (PIPEDA, s. 4(1)(a); *The Constitution Act*, 1867, s. 91(2)). We outline below how "commercial activities" has been understood by the OPC and the courts and its implications for First Nations organizations and businesses.

Personal information about employees that an organization collects, uses or discloses in connection with the operation of federal works, undertakings or businesses is also regulated under PIPEDA (s. 4(1)(b)). This is expressly defined within PIPEDA to mean a work "that is within the legislative authority of Parliament" and the Act provides a non-exhaustive list of examples, including railways, canals, radio broadcasting stations, and banks (PIPEDA s. 2). It is rooted in federal jurisdiction over matters outside of exclusive provincial legislative authority (*The Constitution Act*, 1867, ss. 91(29) and 92(10)). How First Nations organizations may be deemed to be a federal work, undertaking, or business is explored in greater length below.

Before moving to the issues of commercial activities and FWUBs, it is worth noting there are several exceptions to the application of PIPEDA. The legislation does not apply to:

- government institutions subject to the federal *Privacy Act*, which generally means federal departments and agencies,
- individuals insofar as their collection, use or disclosure of personal information is only for personal or domestic purposes, or
- organizations whose collection, use or disclosure is only for journalistic, artistic, or literary purposes.

In addition, when provinces pass "substantially similar provincial legislation" (PIPEDA, s.26(2)) then PIPEDA does not apply to those activities regulated by provincial legislation. These exceptions are summarized in Appendix 1: Exceptions to the Application of PIPEDA.

Commercial Activities

As noted above, PIPEDA applies to an organization that "collects, uses or discloses [personal information] in the course of commercial activities" (PIPEDA, s. 4(1)(a)). In this instance PIPEDA applies "insofar as it relates to how the Canadian economy functions and operates" (*State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada*, 2010 at para. 40). Accordingly, First Nations governments such as Band Councils, as well as First Nations organizations and businesses, may be subject to PIPEDA in relation to their commercial activities (*Witty v Mississauga First Nation*, 2021). It is therefore critical for First Nations to understand how the term 'commercial activities' is interpreted.

Commercial activity is defined in PIPEDA as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists" (PIPEDA s. 2(1)).

The OPC has released a general interpretation bulletin outlining both court and OPC interpretations of commercial activity (OPC, 2017b). It is important to note that while court decisions regarding the interpretation of commercial activity

are precedent setting and must be followed in subsequent cases, the OPC decisions are not. However, OPC decisions are highly persuasive in subsequent cases. We highlight some of the main points below.

The concept of commercial activity is flexible and has shifted to accommodate contemporary commercial practices that may not fit within a traditional understanding of commercial practices as those that contain a buyer, seller, and a commodity. In the modern economy, the most important commodity of many businesses is the information that they collect on their users and then sell to advertisers (*State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada*, 2010 at para. 41).

In determining whether an activity is commercial activity, it is imperative to assess the entire business model, rather than isolated business practices. This was established in *Reference re Subsection 18.3(1) of the Federal Courts Act* (2021). In that case, Google argued that use of their search engine was not commercial activity because it was a free service that simply connected users to information. The court rejected this argument, pointing out Google's highly successful advertising-based revenue model relies on the popularity of the search engine (at para 52-55). This decision exemplifies the pragmatic way that the courts have chosen to interpret commercial activity under PIPEDA. The courts have argued that "the dominant factor" in assessing whether an activity is commercial activity is "the primary characterization" of the activity in question, rather than incidental relationships or forms of conduct (*State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada*, 2010 at para. 106). Thus, a free service, like Google's search engine, can be considered commercial activity, as it is characterized as an essential part of the organization's business model.

OPC decisions follow the business model approach in making decisions surrounding online organizations. In a straightforward case, a company website that is used for advertising the company product is considered to be commercial in nature (PIPEDA Case Summary #2005-305). In a more complex case involving Facebook, the OPC states that personal information falls under PIPEDA, even if it is uploaded by users for their own personal purposes, "to the extent that Facebook uses such personal information in the course of commercial activities" (PIPEDA Report of Findings #2009-008 at para 11). In this decision the OPC further argues that:

> *collection, use and disclosure of personal information in relation to a feature without an apparent direct commercial link can still be characterized as occurring 'in the course of commercial activity' in the sense required under the Act (PIPEDA Report of Findings #2009-008 at para 12).*

The rationale behind the expansive understanding of commercial activity on online platforms is that even those features that lack an obvious connection to Facebook's business model likely still enhance user experience, thus "indirectly contributing to the success of Facebook as a commercial enterprise" (PIPEDA Report of Findings #2009-008 at para 12).

The comprehensive business model approach was reaffirmed in *State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada* (2010), in which the judgment emphasized that PIPEDA's "provisions must be interpreted with and applied with flexibility, common sense and pragmatism" (at para 101). This commonsense approach is exemplified in *State Farm* in determining whether an activity is commercial activity.

In this case, the court stated that if they were to designate the collecting of evidence as commercial in character, as the Privacy Commissioner argues, it would have the absurd consequence of prohibiting "the collection of evidence about a plaintiff by third parties retained by a defendant in response to a tort action" (at para 101). The court rules that this was not the "intention of Parliament in adopting

PIPEDA" and accordingly states that evidence collection in this specific context is not a form of commercial activity (at para 101). Furthermore, the arguably commercial relationships in this case, "are simply incidental to the primary non-commercial activity or conduct at issue" so PIPEDA does not apply (at para 106).

Another case demonstrates the inverse of this approach, wherein the commercial relationship was fundamental to the conduct at issue. In this example, a doctor conducting an independent medical examination for an insurer, was considered a commercial activity under PIPEDA, because the nature of the transaction between the Doctor's corporation and the insurance company was commercial in nature (*Wyndowe v Rousseau*, 2008 FCA 39 at para 35). This is a particularly complex issue. The applicability of PIPEDA to doctor's records relies on (1) the absence of provincial or territorial privacy laws that are deemed 'substantially similar' under PIPEDA and (2) a doctor billing an insurance company for an insurance medical, which may be a relatively rare situation in First Nations communities.

Finally, it is important to note that not-for-profit organizations may be subject to PIPEDA in relation to certain practices that are considered commercial activities. This includes "the selling, bartering or leasing of donor, membership or other fundraising lists" (PIPEDA, s. 2(1)). Having a not-for-profit tax status does not determine whether an organization's data practices are commercial activities for the purposes of PIPEDA (*Rodgers v Calvert* 2004), it is the nature of the activity that is determinative.

First Nations governments, organizations, and individuals engage in many kinds of commercial activities, everything from multimillion-dollar construction companies to gas stations on reserve to the sale of beaded earrings from a home business. These commercial activities may involve the collection of personal information about an identifiable person, such as credit card numbers, phone numbers, and addresses. Generally, PIPEDA will apply, and thus this information must be managed according to PIPEDA (OPC, 2012). The exception is if substantially similar provincial legislation applies, which will be discussed at greater length below.

Federal Works, Undertakings or Businesses (FWUBs)

The text of s.4(1)(b) states that PIPEDA applies to an organization's handling of personal information that "is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."

There are therefore two components to the application of PIPEDA to FWUBs: whether the personal information is employee information, and whether the activity or operation constitutes that of a FWUB.

Employee information

PIPEDA covers employee information collected, used or disclosed by a FWUB. It does not apply to the collection, use, and disclosure of other personal information that may be collected by a FWUB during its business operations. Unless of course it is a commercial activity as discussed above.

For example, PIPEDA protects the personal information of Band Council employees if the Band Council is deemed to be a FWUB. It does not otherwise cover the collection of personal information by the Band Council, for example, about those who live within the First Nations community (*Witty v Mississauga First Nation*, 2021). PIPEDA would not cover, for example, information collected by a Band Council about housing allocations or the provision of student financing. In the *Witty* case, the Federal Court found that the Band was not collecting the information as part of a commercial activity, nor was the complainant, Witty, an employee of the Band. Therefore, PIPEDA did not apply. Note that an organization that is considered a FWUB might collect employee information that is

not about its *own* employees. In that case, PIPEDA would not apply but one of the provincial private sector statutes might apply. This is a complex area of law. It is essential that First Nations governments, organizations, and businesses obtain legal advice to determine what statutes apply, if any.

In distinct circumstances, outlined under s. 7(1)-(3) of PIPEDA, First Nations may collect, use, or disclose the personal information of their employees without their employees' knowledge or consent. These are the general exceptions to consent that also apply to personal information collected, used, or disclosed in the course of commercial activities. For example, an adjudicator may compel a First Nation to disclose an employee's personal information without the individual's knowledge or consent if it is necessary for a legal investigation **(***Fishing Lake First Nation v Paley, 2005*).

In addition, s.7.3 permits that collection, use and disclosure of employee information without consent if the following two conditions are met:

(a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and

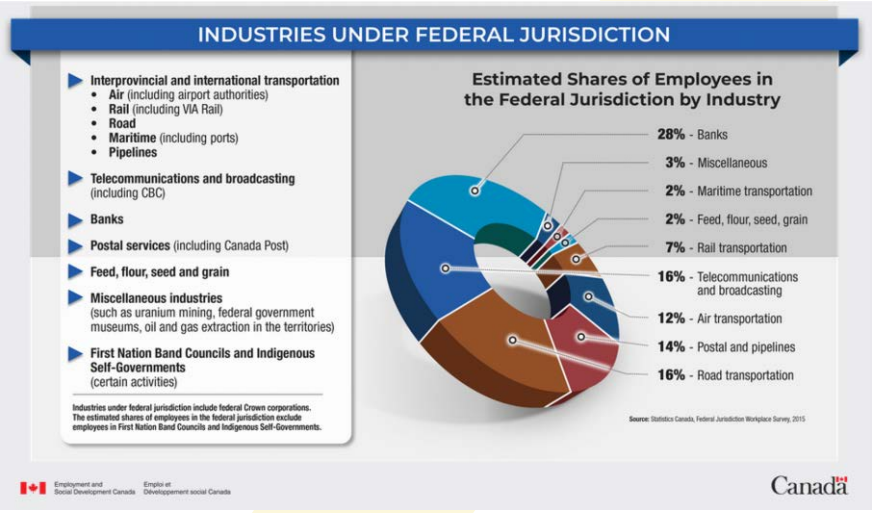
(b) the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.

Operation of an FWUB

The second issue to consider is whether the activity of the work, undertaking or business is "within the legislative authority of federal parliament" (PIPEDA, s.2(1)). As noted in Figure 1 below, this may include First Nation governments. It may also include First Nations service providers and certain First Nations businesses, for example, a railway, radio broadcasting station, bank, etc., or engaged in activities outside the exclusive legislative authority of the provinces (PIPEDA s. 2(1)(i)). Whether PIPEDA applies depends in part on the activities the work, undertaking or business is engaged in while collecting personal information. It's also important to note that a First Nation government may be a FWUB in relation to some activities or departments, but not in relation to others.

The following is an infographic published by Employment and Social Development Canada, outlining industries and activities under federal jurisdiction (Government of Canada, 2022, *Figure 1: Industries under Federal Jurisdiction).*

There is little case law interpreting PIPEDA on this matter that involves First Nations. The same term (FWUB) and definition are used in the Canada Labour Code, however, so it is possible to look to case law in that area to consider how the PIPEDA provision might be interpreted by the Courts. In the Supreme Court of Canada decision in *NIL/TU,O Child and Family Services Society* v. *B.C. Government and Service Employees' Union* ([2010] 2 SCR 696), the Court found that the provision of child and family services, an area of provincial jurisdiction, remained an issue of provincial jurisdiction, despite the fact the service was primarily provided by Indigenous employees to First Nations clients mostly on reserve and the federal government provided most of the funds for the operation of the service. This did not qualify the service as a subject matter



under section 91(24) of the Constitution (Indians and lands reserved for Indians). Rather the tripartite agreement between the federal, provincial, and First Nations governments where it was agreed the provincial government would regulate the service, determined that the matter fell under the provincial labour code. In another instance, however, a First Nation organization that receives most of its funding from a federal government department for the services it provides to a First Nations community was considered a FWUB and therefore PIPEDA applied (PIPEDA Case Summary #2010-004). The fact that the work, undertaking or business is First Nations, does not mean it automatically makes it a matter of federal jurisdiction under section 91(24) of the Constitution. Instead, if it is a subject matter or activity that is governed by the province, for example, labour law, then provincial law applies. Of course, with respect to PIPEDA, not all provinces and none of the territories have legislation that has been deemed substantially similar to the federal legislation. In those cases, PIPEDA applies. Where there is substantially similar provincial legislation, the provincial legislation may apply. The issue of substantially similar provincial legislation is discussed further below. All to say, this is a complex area of law, and it is essential that First Nations get legal advice to ensure they are applying the correct laws.

SUBSTANTIALLY SIMILAR PROVINCIAL LEGISLATION

FWUBs are federally regulated and so will be subject to PIPEDA even if they operate in a province with its own private sector legislation. Alberta, British Columbia, and Quebec have their own private-sector privacy laws that have been deemed substantially similar to PIPEDA. The Governor in Council does this through regulations. (See s. 26(2)(b) and the Exemption Orders made pursuant to this provision: SOR/2004-219, SOR/2004-220, SOR 2003-374). Organizations subject to a substantially similar provincial privacy law are generally exempt from PIPEDA with respect to the collection, use or disclosure of personal information that occurs within that province.

This would apply to both the collection, use and disclosure of personal employee information and the processing of any personal information collected, used or disclosed in the course of commercial activities. Legislation regulating personal health information has also been deemed to be substantially similar in Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador. This paper does not discuss that legislation, further except to note that health privacy legislation generally defines and regulates "personal health information custodians" and their collection, use and disclosure of personal health information. Therefore, individuals and organizations who are not deemed to be personal health information custodians but process some personal health information could still be regulated by PIPEDA, if PIPEDA applies.

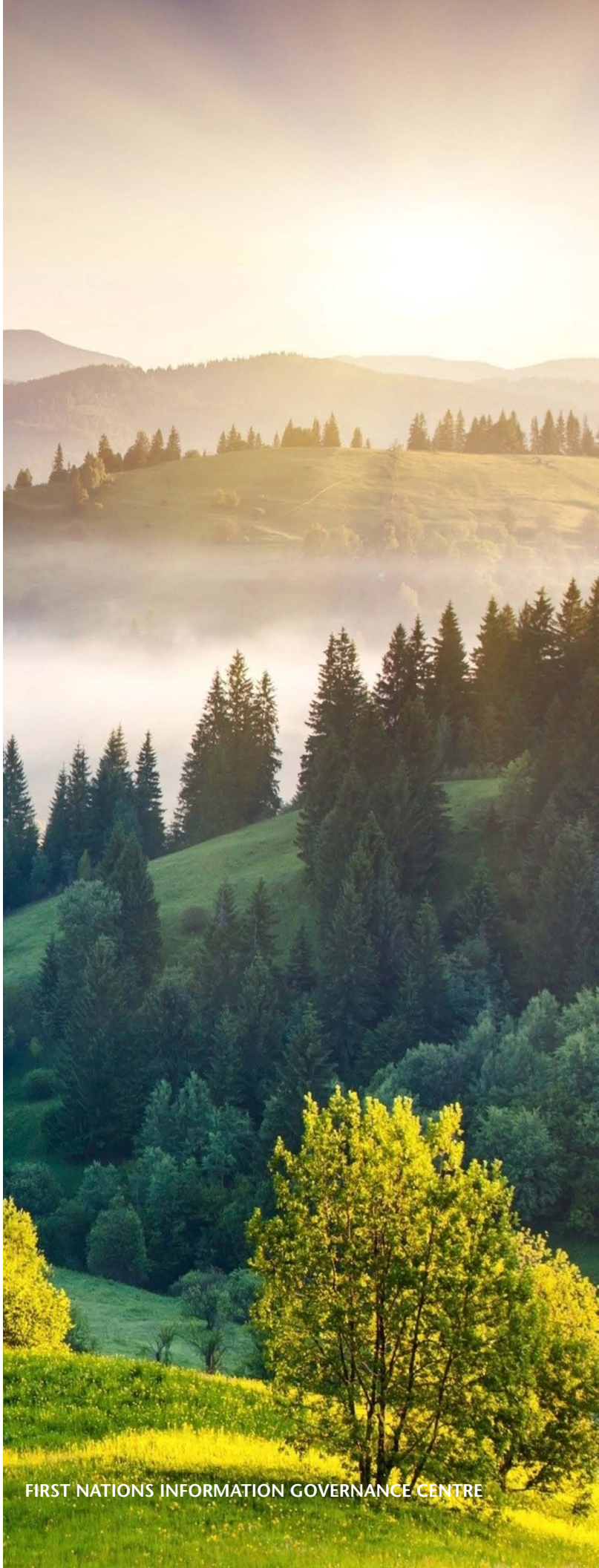
PIPEDA ENFORCEMENT AND INVESTIGATION PROCESSES

The OPC provides many resources that outline the process that begins once a complaint has been filed against an organization (OPC, 2008), and so is not discussed here. An interactive graphic that provides a general overview of the investigation process can be found on the OPC website (OPC, 2017a).

COMPLIANCE CHALLENGES

Complex Jurisdiction Issues

There are many considerations in determining what, if any, privacy laws apply to the various activities of First Nations governments, organizations, and businesses. As has been discussed above, this includes whether the activity is commercial in nature, whether the work, undertaking, or business is a FWUB, whether the personal information respects an employee of a FWUB, and whether provincial laws apply instead of the federal PIPEDA. Consider for example the issue of determining whether an employee of a Band Council is engaged in a FWUB activity or not. If the Band Council is in BC and operating a child and family service, as we saw in *NIL/TU,O*, this is not a FWUB but a provincially regulated activity so PIPEDA would not apply. A Band Council in Manitoba operating the same service, however, might be subject to PIPEDA, because there is no provincial equivalent. Sorting through the jurisdictional complexities is the greatest compliance challenge facing First Nations.



Identifiable Personal Information

PIPEDA regulates personal information, which is defined in s. 2 the Act as "information about an identifiable individual." As the OPC (2019a) outlines, this can include information as various as:

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

The main challenge is to determine what "identifiable" means. The Privacy Commissioner has adopted the interpretation of personal information that was developed in relation to the *Privacy Act*, which is that information is identifiable when there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information (OPC 2013). The key point is that information that has been stripped of direct identifiers (e.g., name) can still be "personal information." The issue of re-identification risks arises with all data protection legislation and is treated similarly across all statutes. Some regulators have created helpful guidance tools, such as the Ontario Information and Privacy Commissioner's *De-identification Guidelines for Structured Data* (2016).

This is an area that can be very technical and where new methods of managing re-identification risks, such as through differential privacy, homomorphic encryption, synthetic data, and other techniques are developing rapidly (Nikolov and Papernot, 2021; Fdal, 2021).

The use of de-identified sensitive information is a matter of concern to First Nations and is discussed below.

Costs

Challenges can arise when organizations adapt their business practices to adhere to existing, or new, privacy legislation. This section briefly outlines three potentially challenging areas of complying with privacy legislation: implementation costs, ongoing compliance costs, and liability for violations.

Implementation Costs

Organizations may need to change their current business practices to comply with data legislation and regulation which can lead to heavy implementation costs (Adam 2021). The diversity of regionally specific privacy legislation forces corporations that operate in multiple jurisdictions to adjust their firms according to these local legal frameworks, further increasing implementation costs (McKinsey 2022). The European Union's early data privacy legislation provides a helpful lens through which to observe the impact of adjusting to new legislation can have on organizations.

The EU was an early adopter of data privacy legislation through the EU Data Directive and its successor, the General Data Protection Regulation (GDPR), which has inspired the adoption of similar legislation internationally (Ardior, Yeon-Koo, Salz, 2020). The GDPR, like PIPEDA, has strong consent requirements and, for this reason, European studies on implementation costs may be informative for Canadian organizations. For example, a 2017 report from the United Kingdom on the implementation of the GDPR anticipated costs of £330-450 ($550 – $750 Canadian) per employee for the implementation of compliance efforts (Sia Partners, 2017).

An American study from 2017 that sampled 53 multinational organizations across varied industries found that the average cost of compliance with data regulations was $5.7 million (Ponemon Institute 2017). Implementation costs increase with the size of the organization as larger operations collect more data, leading to a more complex implementation process (Sia Partners 2017). PwC (PricewaterhouseCoopers) conducted surveys which found that most companies expect increased compliance costs from privacy legislation reform (PwC 2021). About a fifth of surveyed companies estimated that compliance with new legislation would cost their organizations more than $10 million, and the majority of these companies (80%) predicted that data deletion would have the greatest operational impact (PwC 2021).

Though implementation costs are high, studies have shown that the costs of non-compliance are almost three times higher than compliance costs (Ponemon Institute 2017). Non-compliance costs include business disruption, productivity losses, revenue losses, as well as fines, penalties and settlement costs (Ponemon Institute 2017). Therefore, while the initial costs of investing in data compliance may be costly, organizations will likely benefit from such investment in the long run. This is further confirmed by studies on the GDPR which suggests the initial deterrent impact of regulation on the market can be accommodated in the long run (Taufick 2021). Finally, there may be some unexpected benefits for businesses who adhere to privacy legislation. A study of the GDPR points out that privacy legislation that includes a consent provision may make it easier to collect data from those who do opt in, leading to a net benefit for organizations operating under this regime (Ardior, Yeon-Koo, Salz 2020).

Ongoing Compliance Costs

Following the initial investment in adhering to data legislation, it is important for organizations to continue to track the dynamic world of privacy legislation. This is particularly important for companies with offices in different jurisdictions. The costs of complying with data regulations vary widely depending on the local jurisdiction as well as the size and type of the organization (Chander et al 2021). That said, "many organizations face multiple and sometimes competing compliance challenges that require constant monitoring and frequent audits" (Ponemon Institute 2017).

There are two broad impacts of corporate compliance with federal data privacy law: compliance costs and market inefficiencies (Castro, McQuinn 2019). Compliance costs include the following: additional hiring, data protection and enforcement activities, incident response plans, compliance audits and assessments, policy development, and staff certification (Ponemon Institute 2017, Castro McQuinn 2019).

Market inefficiencies are indirect costs that arise from organizations having reduced access to the collection and use of data (Castro, McQuinn 2019). There is also anecdotal evidence demonstrating that privacy and data protection "concerns might have chilling effects on competition" (Taufick 2021). Competition is impacted by regulation because this leads to the lower circulation of data and more stringent rules (Taufick 2021). That said, data regulation may open up new forms of competition as well as allowing firms to compete over business models that address privacy concerns (Brill 2011).

Liability For Violations

Another concern for Canadian organizations is the costs of potential administrative fines if they contravene privacy legislation (Daginis, Dillon 2021). Under the proposed reforms to PIPEDA (which are discussed further in the following section) there are significant penalties for non-compliance with privacy legislation ranging from administrative remedies to fines to criminal penalties, for a narrow subset of provisions (Baker McKenzie 2022). Enforcement of PIPEDA is much weaker as the Privacy Commissioner can not issue orders or impose financial fines or penalties. However, there are a number of specific offences under PIPEDA (s.28) and organizations that commit these offences may be subject to fines of up to $100,000 CD (Baker McKenzie 2022). The Federal Court can also award damages to a complainant if they appeal to the court following an investigation (OPC 2015).

Other costs associated with violating privacy legislation include compliance monitoring by the Office of the Privacy Commissioner (OPC), seen most clearly through the six-year compliance agreement between the OPC and Equifax (OPC 2020). As part of this agreement, Equifax must "submit third party security audit reports, improve their accountability and data destruction programs, and increase transparency about their privacy practices" (OPC 2020).

CURRENT LAW REFORM PROPOSALS: BILL C-27

On June 16, 2022, the Federal government introduced Bill C-27, the *Digital Charter Implementation Act*. This Act introduces three new pieces of legislation: privacy legislation meant to replace PIPEDA, legislation creating a new Data Protection Tribunal, and legislation that regulates some of the potential harms associated with artificial intelligence (AI). This section primarily discusses the proposed new privacy legislation, the Consumer Privacy Protection Act (CPPA).

Key Similarities

The new legislation's scope of application is quite similar to PIPEDA's and uses almost identical language in this area. Both acts apply to the collection, use, and disclosure of personal information in the course of commercial activities or related to employees and job applicants in connection with the operation of a federal work, undertaking or business. Similarly, both acts are explicit that they do not apply to government institutions to which the *Privacy Act* applies, or information used for personal, domestic, journalistic, artistic, or literary purposes. Both acts use essentially the same definition of personal information: "information about an identifiable individual."

The core provision of PIPEDA, s. 5(3), which limits the collection, use, and disclosure of personal information to matters and purposes that "a reasonable person would consider appropriate in the circumstances" is replicated identically in s.12(1) of the new legislation.

Both pieces of legislation require an organization to obtain an individual's consent before collecting, using, or disclosing their personal information, subject to specific exceptions. Many of these exceptions from PIPEDA are reproduced in the new legislation, including:

- the exceptions for investigating the contravention of a law of Canada, a province, or foreign jurisdiction,
- for publicly available information specified in the associated regulations,
- for research purposes,
- for when collection, use or disclosure is required by law,
- for disclosure to government institutions under certain circumstances, or
- for certain emergency circumstances that threaten the life, health or security of an individual.

A comparison between these key elements is summarized in Appendix 2: Comparison of PIPEDA and CPPA.

Key Differences

Despite the similarity between PIPEDA and CPPA regarding the key elements for governing the collection, use and disclosure of personal information, there are also differences. These are summarized below.

Consent

CPPA imposes additional requirements for organizations to meet for an individual's consent to be valid for the collection, use, or disclosure of their personal information. Specifically, individuals must be made aware of the type of personal information that is to be collected, used, or disclosed as well as the names of third parties to which the personal information may be disclosed. The new legislation also stipulates that necessary information to obtain consent must be communicated to the individual in plain language, such that the individual would reasonably be expected to understand. Lastly, the new legislation requires the organization to obtain the individual's consent before or at the time of collection and makes express consent the default form of required consent.

Transparency

In addition to clarifying the consent provisions, the CPPA includes more stringent transparency requirements. Businesses and FWUBs' policies and practices must be available in "plain language" (s.62) and, where automated decision systems are used there are obligations of transparency (s.62(2)(c)) and explanation (s.63).

Minors

The CPPA includes new protections for minors. The most important is that the personal information of minors is considered sensitive (s. 2). There are heightened obligations in relation to sensitive information. For example, in applying appropriate purposes, form of consent, retention and disposal, data breach notification, de-identification measures, and privacy management programs.

Exceptions to Consent

Another important difference between PIPEDA and CPPA is the introduction of a variety of new exceptions to the consent requirement for the collection, use, or disclosure of personal information related to "business operations" in CPPA. These exceptions include one for: "business activities" where "a reasonable person would expect the collection or use for such an activity" (s.18(2)) and for pursuing an organization's legitimate interest that "outweighs any potential adverse effect on the individual resulting from that collection or use" (s.18(3)). First Nations will want to consider how these exceptions to consent are interpreted and their implications to their data sovereignty in the years to come.

Regulation of De-identified Information

There are also new exceptions to the consent requirement when dealing with "de-identified" personal information. These include the use of de-identified information for internal research, analysis, and development (s.21), prospective business transactions (s.22), and the disclosure to some types of organizations for "socially beneficial purposes" (s.39).

The CPPA defines de-identify as "to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains" (s.2). It also defines anonymize as "to irreversibly and permanently modify personal information" so that there is no risk of re-identification (s.2). Therefore, unlike PIPEDA, for data processing activities to fall outside the regulatory ambit of the legislation an organization must meet the stringent definition of anonymize. Otherwise, these activities will be regulated. However, if the personal information is de-identified then it might be treated differently than personal information.

There are also provisions that require that measures to de-identify information are proportionate to the sensitivity of the information (s.74) and that prohibit an organization from taking steps to re-identify information, subject to some exceptions (s.75).

De-identifying sensitive information (such as banking records, health information, etc.) still permits the data holder to use First Nation identifiers and to aggregate data based on First Nation status. This will run afoul of the First Nations Principles of OCAP®. Where de-identification is permitted, First Nations may prefer a restriction on the use of de-identified information so that it could not be used for the purpose of conducting research that involves First Nations as a focus of interest unless the research is conducted in compliance with OCAP® principles. For example, consent is still required for the use of First Nations de-identified information.

Compliance, Penalties and Enforcement

The CPPA sets out a regime for creating codes of practice as well as certification programs (ss. 76-81). This can potentially diminish the uncertainty involved in complying with the legislation.

The CPPA includes new and significant penalties for breach of its obligations, although these new penalties do not apply to all obligations (s.94). There is also a private right of action (s.107). In addition to these penalties, the CPPA introduces a number of new offences (s.128).

There are new requirements as well regarding audits (s.97), creating a privacy management program (s.9), and providing documentation to the Privacy Commissioner regarding this program (s.10).

Data Portability

The CPPA creates a framework for data portability whereby an individual can request that an organization disclose her personal information to another organization (s.72). Both organizations have to be covered by a data mobility framework, the details of which are left to be developed in regulations under the legislation (s.123).

CHAPTER TWO: FIRST NATIONS DATA SOVEREIGNTY AND LAW REFORM

FIRST NATIONS DATA SOVEREIGNTY AND CANADIAN PRIVACY LAWS

Since time immemorial, First Nations people have occupied and governed themselves and their territories within what are now the boundaries of Canada. As sovereign nations, many entered into treaty relations with the Crown. Currently, Treaty Rights along with other rights are recognized by s. 35 of the Constitution Act, 1982, which states that "the existing aboriginal and treaty rights of the aboriginal peoples of Canada are hereby recognized and affirmed."[1] The Quebec Court of Appeal recently held that s.35 recognized and affirmed an inherent right to self-government.[2] The 2000 Campbell decision by the BC Supreme Court also concluded that s.35 protected the inherent right to self-government (Campbell et al v AG/BC/AG Cda & Nisga'a Nation et al., 2000, Sga'nism Sim'augit (Chief Mountain) v Canada (Attorney General), 2013).

Data sovereignty is an integral component of the achievement of First Nations self-government and self-determination. Access to data is essential to governance. As the First Nations Information Governance Centre (FNIGC) has pointed out "First Nations governments require timely access to quality data to plan, manage, and account for investments and outcomes associated with their citizen's well-being" (2020, p.3). Connected to this is a desire to "embrace the challenges and opportunities of a 21st century marked by digital revolutions" (2020, p.85). But data sovereignty also means sovereignty over data practices, or "managing information in a way that is consistent with the laws, practices and customs of the Nation or State in which it is located" (Snipp, 2016).

In furtherance of the goal of data sovereignty, FNIGC has introduced a First Nations Data Governance Strategy. It is based on eight guiding principles: Community-driven and Nation-based, OCAP®, Relationships, Transparency and Accountability, Quality Community-driven Standards and Indicators, Nation (Re)Building, Equity and Capacity, Effective Technology and Policy. The implementation of the strategy is organized around nine pillars.

1 "Aboriginal peoples" is defined as including "Inuit, Indian, and Métis people". Currently, the term "Indigenous" is generally used instead of "Aboriginal" and this report adopts this usage when needing to use a general umbrella term. Throughout most of this report we use the term "First Nations", which does not include Inuit or Métis peoples.

2 Reference to the Court of appeal of Quebec in relation with the Act respecting First Nations, Inuit and Métis children, youth and families. Note that the federal government is appealing this decision, not because of a disagreement with this general finding, but because of issues regarding the relative roles of federal and provincial jurisdiction. See: https://www.canada.ca/en/indigenous-services-canada/news/2022/03/the-government-of-canada-appeals-the-quebec-court-of-appeals-opinion-on-the-act-respecting-first-nations-inuit-and-metis-children-youth-and-families.html

The first two pillars, First Nations Data Governance and First Nations Digital Infrastructure, are cross-cutting and address the need for regional centres that are integrated to some degree and that provide support for First Nations data stewardship needs, including managing privacy and confidentiality (2020, p.8).

The remaining seven pillars reflect specific functions:

- Rights Holder Relationship Management,
- First Nations Data Access and Repatriation,
- First Nations Data Collection, Discovery, and Gap Bridging,
- First Nations Data Standards and Intergovernmental Interoperability,
- First Nations Data Management,
- First Nations Data Trust, Ethics, and OCAP® implementation,
- Data Relationship Management with Other Levels of Government and Partners.

This broad agenda encompasses more than privacy issues. It is important to note that First Nations data sovereignty applies to a very broad range of data. As FNIGC describes it:

> *It is First Nations' intellectual property, historic and contemporary data, survey data, administrative data, and data from alternative sources, including data generated through research activities. It includes but is not limited to data about lands, resources and environmental data "about us" such as demographic, socio-economic and health, housing, infrastructure, and other services, as well as data "from us" … such as our languages, cultures, knowledge, and stories (2020, p.2).*

This is a much broader category of data than the personal information that is regulated by Canadian privacy laws.

Pillar 8 refers to the First Nations Principles of OCAP®. The principles of ownership, control, access, and possession are described as follows (FNIGC, 2022):

> **Ownership** refers to the relationship of First Nations to their cultural knowledge, data, and information. This principle states that a community or group owns information collectively in the same way that an individual owns his or her personal information.
>
> **Control** affirms that First Nations, their communities, and representative bodies are within their rights to seek control over all aspects of research and information management processes that impact them. First Nations control of research can include all stages of a particular research project-from start to finish. The principle extends to the control of resources and review processes, the planning process, management of the information and so on.
>
> **Access** refers to the fact that First Nations must have access to information and data about themselves and their communities regardless of where it is held. The principle of access also refers to the right of First Nations' communities and organizations to manage and make decisions regarding access to their collective information. This may be achieved, in practice, through standardized, formal protocols.
>
> **Possession** While ownership identifies the relationship between a people and their information in principle, possession or stewardship is more concrete: it refers to the physical control of data. Possession is the mechanism by which ownership can be asserted and protected.

These are principles that speak to the issue of control over data but not in the sense in which this is understood in Canadian privacy law. First, data as defined here includes much more than personal information. Second, data sovereignty for First Nations is not an issue of individual control but

community control—it is about collective rights to self-determination and self-governance rights. Community rights in data and protections for personal privacy rights need to work together. The ideal is that the protection of community rights will increase protection of personal data, adding another layer of protection to personal information.

Even if Canadian privacy laws are only one element to examination in achieving the goals of First Nations data sovereignty, they are an important element. Canadian privacy laws such as the *Privacy Act* (regulating the public sector) and PIPEDA (regulating the private sector) create a framework of what the courts have called "quasi-constitutional" legislation regulating the collection, use and disclosure of personal information.

Moreover, the *Privacy Act* is meant to work together with the *Access to Information Act* in the treatment of personal information. In the provinces and territories, public sector privacy law and access to information (or freedom of information) are combined into one piece of legislation instead of two and many provinces also have legislation pertaining specifically to personal health information. Many of the pillars of the First Nations Data Governance Strategy involve issues regulated by privacy and access to information laws. Privacy is explicitly mentioned in the descriptions of pillars 1, 2, 6, and 8.

Pillar 4, which is about data access and repatriation, is also relevant as privacy laws often involve legislative and other pathways for governments, and other organizations, to gain access to data. Pillar 5, which addresses the creation of data linkages combining multiple sources of data and control over research that impacts First Nations communities, can also be affected by privacy laws. Finally, pillar 9 outlines the need for multi-jurisdictional data governance, the devolution of services, and the role of data sharing and linkage projects—all of which can be impacted by privacy laws. The remaining two pillars, 3 and 7, speak to the existence of capacity to support First Nations with their data priorities and data management. Many of these functions could intersect with privacy law concerns as well.

Below, this report outlines how PIPEDA—and the proposed reforms to PIPEDA—affect this vision of First Nations data sovereignty. In particular it will outline tensions and inconsistencies concerning:

- the lack of recognition of First Nations governments,
- the lack of First Nations control over data related to their communities for research purposes, or other "social good" purposes,
- the individual focus of privacy law, which might be in conflict or tension with some First Nations norms, and
- capacity-building needs.

Before turning to this analysis in more detail, the following section outlines Canada's obligations under UNDRIP and argues that addressing these shortcomings in Canadian privacy law is now an obligation of the federal government.

UNITED NATIONS DECLARATION ON THE RIGHTS OF INDIGENOUS PEOPLES

In 2007, the UN General Assembly adopted the *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP). In 2021, the federal government passed the *United Nations Declaration on the Rights of Indigenous Peoples Act* (UNDA). The Act requires the Government of Canada to take all measures to ensure that Canadian laws are consistent with the Declaration (s.5), and to prepare and implement an action plan to realize the objectives of the Declaration and monitor progress (s.6). Its preamble also affirms that UNDRIP is "a source for the interpretation of Canadian law."

UNDRIP includes important principles that are relevant to the issue of First Nations data sovereignty. First, several principles speak to First Nations' inherent rights of self-determination (Article 3) and self-government (Article 4). Also included is the right to development (Article 23). As outlined in the previous section, First Nations governments require access to data in order to govern and exercise other rights.

The full and effective application of UNDRIP and the opportunity for First Nations to fully realize their rights, requires legislative and other pathways for First Nations access to data needed to govern. It also requires First Nations consent to legislation that affects First Nations. Article 19 outlines the requirement of free, prior and informed consent (FPIC) before "adopting and implementing legislative or administrative measures that may affect them." Further, Article 5 recognizes and protects Indigenous institutions by stating that:

> *Indigenous peoples have the right to maintain and strengthen their distinct political, legal, economic, social and cultural institutions, while retaining their right to participate fully, if they so choose, in the political, economic, social and cultural life of the State.*

This is further supported by Article 34, which recognizes the right to institutions and traditions, including juridical systems.

Data practices that are reflective of the unique world views of First Nations can also be considered part of the right to their own cultural heritage, protected by Articles 12, 13, and 31. Article 31 states:

> *Indigenous peoples have the right to maintain, control, protect and develop their cultural heritage, traditional knowledge and traditional cultural expressions, as well as the manifestations of their sciences, technologies and cultures, including human and genetic resources, seeds, medicines, knowledge of the properties of fauna and flora, oral traditions, literatures, designs, sports and traditional games and visual and performing arts. They also have the right to maintain, control, protect and develop their intellectual property over such cultural heritage, traditional knowledge, and traditional cultural expressions.*

While the examples refer to traditional scientific knowledge and cultural property, these examples are non-exhaustive. Privacy, and other data norms, is deeply connected to culture. Privacy laws should not be considered "universal" but rather reflective of cultural and political choices regarding the nature of the value of privacy and how it should be balanced against other important values. As Williams et al. point out, Canadian data laws rely upon understandings of privacy that are highly individualistic whereas First Nations understandings would include communal ideas of privacy (2011).

Moreover, what types of information are seen to carry a strong privacy interest can vary. Gee argues that for Indigenous communities, "retaining privacy over certain traditional cultural practices is a long-established convention based on an understanding of collective privacy" (2019). Health, education, financial, and social indicators data and information is also sensitive, and is data that can be used to harm a First Nation intentionally or unintentionally.

Finally, Article 39 supports the view that the government is obliged to provide support for capacity building regarding data sovereignty. It states that "Indigenous peoples have the right to have access to financial and technical assistance from States and through international cooperation, for the enjoyment of the rights contained in this Declaration." Financial and technical assistance to support First Nations in the application of federal and provincial privacy laws might be welcome by First Nations.

Although the federal government, under UNDA, is obligated to ensure that its legislation is consistent with the principles of UNDRIP, this has so far had little impact on privacy law reform efforts. The introduction of Bill C-27, which would replace PIPEDA with the new CPPA, includes nothing that refers to the goals of Indigenous data sovereignty. This is even though in its report regarding its original set of consultations on the Digital Charter, the government indicated that it heard from Indigenous Peoples regarding the importance of the goals of Indigenous data sovereignty, respect for frameworks like the First Nations Principles of OCAP®, and the need to implement UNDRIP (Innovation, Science and Economic Development Canada, 2019).

In its discussion paper regarding *Privacy Act* reform, the federal government does indicate that one of its goals is to advance reconciliation with Indigenous peoples (Department of Justice Canada, 2020, p. 3). The proposals, which are general, focus on creating better mechanisms for sharing data with Indigenous governments, new protections when the personal information about Indigenous persons is at issue, and consideration of communal privacy protection. However, two main issues are missing.

The first is any kind of framing in terms of data sovereignty and the need for Indigenous data to be governed by the laws, traditions, and practices of Indigenous communities. Although communal privacy protection is meant to reflect Indigenous views regarding individual and communal privacy, the point should be to allow communities to determine data norms for themselves and to create legislative and other pathways for the recognition and integration of such norms.

The second missing issue is the acknowledgement that both the *Privacy Act* and PIPEDA require reform and that their reform should be considered together. The federal government should not seek a more fulsome definition of Indigenous governments in the *Privacy Act*, for example, while still regulating some of First Nations' data practices under PIPEDA (i.e., personal employee information) and failing to recognize them as government institutions for other purposes under PIPEDA (see further discussion of this matter below).

At the provincial level, in 2019 the BC government passed the *Declaration on the Rights of Indigenous Peoples Act* which obligates the provincial government: to ensure that its laws are consistent with UNDRIP, to create and implement an action plan to achieve the UNDRIP's objectives, to monitor progress, and to allow the province to enter into agreements with Indigenous governments and share statutory decision-making.

In 2022 BC released its *Declaration Action Plan*, which includes two provisions that are directly relevant to First Nations data sovereignty:

> *3.14 Advance the collection and use of disaggregated demographic data, guided by a distinctions-based approach to Indigenous data sovereignty and self-determination, including supporting the establishment of a First Nations-governed and mandated regional data governance centre in alignment with the First Nations Data Governance Strategy.*
>
> *3.15 Adopt an inclusive digital font that allows for Indigenous languages to be included in communication, signage, services and official records.*

Missing from this plan is any examination of provincial privacy laws for their consistency with the Declaration. The recent decision by the Information and Privacy Commissioner of BC denying several First Nations governments access to health information they requested to help them better manage Covid-19 highlights the need for such legislative review (OIPC, Order F20-57). This report will not discuss the reform of provincial legislation, but it is important as part of the broader agenda for First Nations data sovereignty.

PRIVACY LAW REFORM

The Need for Comprehensive Federal Privacy Law Reform

The implementation of UNDRIP requires comprehensive legislative review and reform of Canada's privacy and access to information laws to ensure that First Nations governments can exercise their right of data sovereignty.

One of the central issues with the current regime is that First Nations governments are included (partially) in laws that regulate the federal private sector rather than the federal public sector. As has already been outlined in Chapter One, some, but not all, and in fact, less and less employee personal information that is collected, used or disclosed by First Nations governments, such as Band Councils, falls within PIPEDA. Apart from employee information, the collection, use and disclosure of other personal information by First Nations governments is not regulated by either PIPEDA or the *Privacy Act*. What is ultimately needed are First Nations laws.

The Need for Financial, Technical and Legal Support

There is a need to build capacity for First Nations to craft their data laws. Whatever form these laws take, there will also be the need for capacity to manage data that might be subject to multiple jurisdictions. It is likely that whatever data norms are reflected in First Nations laws there will also be the need to determine issues such as re-identification risks and security risks. These are highly technical areas that require technical-capacity building in addition to legal-capacity building.

There are capacity-building needs associated with the interim measures discussed in the following sections as well. As Chapter One of this report discussed, the costs of complying with privacy legislation like PIPEDA can be considerable. The proposed CPPA would shift federal privacy law from its current Ombuds-model to one where the Privacy Commissioner has stronger powers, including the power to recommend fines and penalties. The threat of new penalties and fines could also affect contracting-out decisions. Just as under PIPEDA, organizations can use service providers for their

data processing needs but the organization remains responsible for compliance with the legislation.

Article 39 of UNDRIP outlines the right to "to financial and technical assistance" for the enjoyment of UNDRIP rights. First Nations data sovereignty does not just require law reform, but the assistance needed to both achieve and fully realize the needed reforms. The full and effective application of UNDRIP and the opportunity for First Nations to fully realize their rights, requires recognition of First Nations right to data sovereignty and the capacity to fully exercise that right.

Interim Measures and PIPEDA Reform

As discussed earlier in this report, the federal government has already proposed reforms to PIPEDA with the introduction of Bill C-27. If passed, Bill C-27 would enact the CPPA to replace PIPEDA. In the following discussion we focus on the proposed CPPA rather than PIPEDA but will outline through several tables which aspects of the CPPA are shared with PIPEDA (or are substantially similar) and which are unique to CPPA.

Legislative and Other Pathways for Recognition of First Nations Laws

The CPPA, like PIPEDA, applies to commercial activities within Canada. However, where provinces pass legislation that is "substantially similar" the Governor in Council can pass regulations recognizing this and exempting the application of the CPPA within that province (s. 122(2) and (3)). First Nations, however, hold inherent and Treaty rights recognized under section 35 of the Constitution. First Nations do not need the federal government to pass legislation recognizing this right, instead the CPPA needs to be amended to ensure it does not interfere with First Nations rights or the application of First Nations laws. First Nations exemption from the application of the CPPA should not have to meet the substantially similar test, because the basis for opting-out is the inherent First Nations rights of self-government and self-determination in accordance with their own distinct worldviews. Applying the substantially similar test would make the federal law the benchmark.

First Nations jurisdictions would not only be potentially exempt from the application of the CPPA but should also fall under a different mechanism for data protection and privacy oversight and accountability, generally. The current proposed structure for enforcing these laws through the Commissioner and Tribunal raises further questions for building a data governance framework that adheres to the principles of First Nations data sovereignty. It is entirely inconsistent with those principles to have those policies enforced by a Federal Commission and Tribunal without any provisions being made in the enabling statutes for adequate consideration of Indigenous perspectives or Indigenous data sovereignty in the operations and decisions of those bodies. Indeed, this is a potential problem for any of the proposed interim measures towards meaningful First Nations data sovereignty. First Nations might consider the value of establishing a First Nations privacy commissioner and tribunal to govern themselves.

For First Nations, there is also a concern about the existing gap in the legislation where de-identified (aggregated) information loses all protections under PIPEDA and all privacy legislation. CPPA should be amended to prevent the use of de-identified data if the result is an aggregation of data about individual First Nations communities, groups of First Nations communities or First Nations in general, without the consent of the respective community, government, organization, etc. This would allow the application of the First Nations Principles of OCAP® - ownership, control, access, and possession - to information held outside First Nations communities without their free, prior, and informed consent. This amendment also should be made to the federal *Privacy Act*.

There are many aspects of privacy law that are culturally and politically specific to particular jurisdictions. For example, the value of individual privacy has been linked to other concepts as diverse

as autonomy, freedom, intimacy, identity, and trust. In all privacy laws, privacy is also balanced against other social and political values and goals to determine its limits. In addition to this value-laden balancing, privacy laws currently do not reflect group interests in data – considerations of harm, sensitivity, and reasonable expectations all reflect individual interests. Given this, First Nations data laws might make different choices than statutes like the CPPA.

The following Table provides several (non-exhaustive) examples where the CPPA takes a strong individual focus in several provisions.

Table 1: Individual Focus of CPPA

Provision of CPPA	Individual Focus
Appropriate Purposes (s.12)	• Obligation is in addition to consent • Factors include: sensitivity of the information (s. 12(2)(a)), proportionality of individual loss of privacy (s. 12(2)(e))
Legitimate Interest (s.18(3)) *New in CPPA*	• Exception to knowledge and consent • Consideration of "adverse effect on the individual", expectations of a "reasonable person" and whether the purpose is to influence "individual's behaviour or decisions"
Business Activities (ss. 18(1) and (2)) *New in CPPA*	• Exception to knowledge and consent • For purpose of listed business activity (s.18(2)) • Consideration of expectations of a reasonable person and whether purpose is to influence "individual's behaviour or decisions"
Individual's Interest (ss. 29(1) and (2)) *Expanded to include use in CPPA*	• Exception to knowledge and consent • In cases where collection is "clearly in the interests of the individual and consent cannot be obtained in a timely way"

The CPPA, like PIPEDA, requires that any collection, use or disclosure of personal information be only conducted for purposes and in a manner that a reasonable person would consider appropriate in the circumstances (s.12(1)). The CPPA lists several factors that must be considered in determining the appropriateness of a purpose or manner (s. 12(2)). Amending the legislation to add another factor which specifies Indigenous data sovereignty and Indigenous conceptions of privacy could be another viable means of enacting meaningful First Nations data governance through the CPPA.

The "legitimate interests" exception to knowledge and consent is a compelling example of the tensions between current Canadian privacy and information governance and First Nations data sovereignty. Under this exception, businesses can avoid the consent requirement by identifying a mere legitimate interest in the data, whereas First Nations organizations are not provided with any means to access their right, as per UNDRIP, to exercise sovereignty over their own data. Resolving this tension may require amending the 'legitimate interests' exception to stipulate that legitimate interests includes implementation of the principles of Indigenous data sovereignty where the personal information at issue is associated with an Indigenous person.

Codes of Practice Tailored to First Nations

The CPPA introduces a new regime where the Privacy Commissioner can approve of codes of practice that provide "substantially the same or greater protection of personal information as some or all of the protection provided under this Act" (s. 76). The Privacy Commissioner can also approve of certification programs that would create mechanisms for organizations to verify that they are compliant with approved codes of practice (s.77).

This provides an important potential pathway for creating codes of practice that are specific to First Nations organizations that are regulated by the CPPA. Because these codes of practice must offer the same level of protection as the CPPA, they will not necessarily be fully reflective of First Nations laws, traditions, and practices. However, this remains an important interim step toward First Nations data sovereignty. It could be that further changes to the CPPA be proposed which would support interpreting the CPPA in light of the goals of Indigenous data sovereignty and UNDRIP. This might provide a means to interpret terms like "sensitive," "reasonable expectations" and "appropriate purposes" in a manner that is more culturally appropriate.

It is important to note that both codes of practice and certification programs can be proposed by an "entity," which is understood to include organizations and government institutions not regulated by the CPPA. For example, with adequate funding the First Nations Information Governance Centre could create supports for the creation of community-specific codes of practice. A First Nations entity could be mandated to independently certify compliance with those codes of practice.

Recognition of First Nations Governments as Government Institutions

The CPPA includes several exceptions to the requirement of knowledge and consent that make reference to government institutions or the laws of Canada or the provinces. These are listed in Table 2 below.[1]

However, it is unlikely that these exceptions would include First Nations governments and laws for at least two reasons. First, legislation like the CPPA continues to treat Band Councils and other First Nations Self-Governments as part of the federally regulated private sector. Second, public sector privacy legislation, like the *Privacy Act*, adopts explicit language referring to "aboriginal governments" when outlining similar exceptions, but only a few First Nations governments that have entered into self-government agreements are recognized as "aboriginal governments" under this legislation. This suggests that if other federal data protection legislation does not adopt such explicit language, then First Nation governments are not understood to be included in "government institution."

Because of this structure, First Nations governments are deprived of some legislative pathways for obtaining information from the private sector that are available to other levels of government. However, simply adding First Nations governments to these exceptions creates its own complexities because they are currently not subject to comprehensive privacy law obligations and oversight that would govern the information they collect from private sector organizations.

Solving this requires a long-term comprehensive approach, recognizing First Nations rights to data sovereignty for self-determination and self-government. There are several examples of First Nations privacy laws and policies in British Columbia that could be built upon, including the Tla'Amin First Nation *Freedom of Information and Protection of Privacy Act* (2016), the Tsawwassen First Nation *Freedom of Information and Protection of Privacy Act* (2009), the Westbank First Nation *Freedom of Information and Protection of Privacy Law No, 2018* (2018), the Mamalilikulla First Nation *Privacy Policy* (2020), as well as numerous examples specific to the research context.

1 Note that some of these provisions refer to exceptions to knowledge and consent for the "disclosure" of personal information and some also refer to "collection" and/or "use". We have omitted those details in the chart.

Table 2: Reference to government institutions or the laws of Canada or the provinces in CPPA

CPPA Provision	Language Used
Identification of Injured, ill or deceased individual (s. 31)	"Government institution"
Communication with next of kin of injured, ill or deceased individual (s. 33)	"Government institution" "lawful authority"
Where individual may be the victim of financial abuse (s. 34)	"Government institution"
Socially beneficial purposes (s. 39) - *New in CPPA*	"government institution" – but also lists "other prescribed entity" which could potentially include First Nations governments(1)(b)(iv)
Breach of agreement or contravention of law (s. 40)	"Federal or provincial law" "law of a foreign jurisdiction"
Purpose of administering law (s. 43)	"Government institution" "federal or provincial law"
Law enforcement where requested by government institution (s. 44)	"government institution" "lawful authority" "federal or provincial law or law of a foreign jurisdiction"
Contravention of law (s. 45)	"Government institution" "federal or provincial law or law of a foreign jurisdiction"
Proceeds of Crime and Terrorist Financing Act (s. 46)	"Government institution" (as referred to in the Act)
National security, defence or international affairs (ss. 47 and 48)	"Government institution" "lawful authority"

Control Over First Nations Data

The CPPA includes several new exceptions to knowledge and consent that affect the level of control First Nations have over data about their citizens and communities. Some of these exceptions permit the disclosure of "personal information" without knowledge or consent. Some of these exceptions permit the disclosure of "de-identified information" without knowledge or consent. We summarize these exceptions in the chart below.

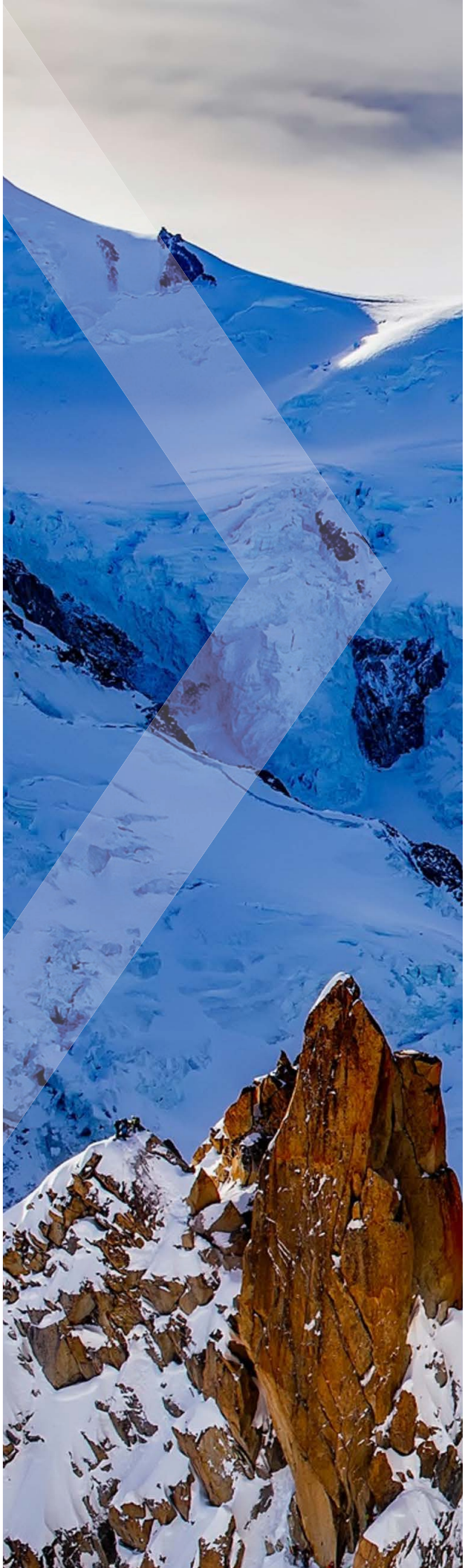
The first four exceptions listed—those that pertain to personal information—are in tension with the goals of First Nations data sovereignty as they create legislative pathways for access to information about First Nations citizens that are inconsistent with the OCAP® principles and which are being proposed without First Nations free, prior, and informed consent. These all already exist in PIPEDA.

The exemptions to de-identified information can still reveal population-level insights and so are a concern to First Nations. It is also the case that First Nations might want access to de-identified information held by private sector organizations in order to gain their own population-level insights.

These provisions as they stand are inconsistent with Canada's obligations under UNDRIP and require amendment. One example to look to might be BC's new *Anti–Racism Data Act*, which has several provisions requiring consultation and collaboration with Indigenous peoples. Another possible solution to this issue would be the previously discussed amendment to s.12 instructing courts to be mindful of the principles of First Nations data sovereignty and conceptions of privacy in determining what purposes for and manners of collection are appropriate. With this amendment, collection, use, or disclosure of personal information about First Nations citizens that is inconsistent with the OCAP® principles could be restricted as not fulfilling the appropriate purposes and reasonable manner requirements, regardless of whether or not an exception to consent could be applied.

Table 3: CPPA Exemptions

CPPA Provision	Requirements
Disclosure for statistical, study or research principles (s. 35)	• Impracticable to obtain consent • Privacy Commissioner is informed
Disclosure to institution for the purpose of conservation of records of historic or archival importance (s. 36)	• Institution's function must include conservation of such records
Disclosure after a period of time (s. 37)	• 100 years after record was created or 20 years after death of individual, whichever is earlier
Journalistic, artistic or literary purposes (s. 38)	• Must be solely for these purposes
Use for internal research, analysis and development (s. 21) New in CPPA	• De-identified information specific to First Nations can only be used with FN consent.
Disclosure for socially beneficial purposes (s.39) New in CPPA	• De-identified information • Disclosure to a government institution, health care institution, post-secondary educational institution, public library, organization that by law or contract with a government institution carries out a socially beneficial purposes, or a "prescribed entity" (s.39(1)(b) • a socially beneficial purpose is defined as "a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose" (s.39(2))



CONCLUSION

With the introduction of Bill C-27, the federal government is proposing to replace PIPEDA with new privacy legislation, the CPPA. Unfortunately, neither PIPEDA nor the CPPA advance First Nations data sovereignty. As this report has argued, this failure makes Canada's privacy law reform efforts inconsistent with the principles of UNDRIP, principles that Canada is now obligated to implement. In particular, both PIPEDA and the proposed CPPA suffer from a number of deficiencies, including:

- the lack of First Nations control over data related to their communities for research purposes, or other "social good" purposes,
- The lack of First Nation governance over aggregate data about First Nations;
- the individual focus of privacy law, which might be in conflict or tension with some First Nations norms,
- the use of de-identification methods to evade all privacy protections and expose First Nations data to unauthorized use or disclosure, and
- capacity-building needs.

This Issue Paper has offered a number of suggestions where the CPPA could be amended to be more responsive to First Nations data sovereignty. Ultimately what is needed are First Nations data laws. However, there are interim steps on the path towards that goal and some of these steps should involve reforming Canada's existing privacy laws.

REFERENCES

Aridor, Guy; Che, Yeon-Koo; Salz, Tobias. (2020). *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3522845

An Act respecting the protection of personal information in the private sector [R.S.Q. 1994], P-39.1. https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1

Baker McKenzie. (2022). Penalties for Non-Compliance. *Global Data Privacy and Security Handbook.* https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/north-america/canada/topics/penalties-for-non-compliance

Bill C-11: An Act to amend the Broadcasting Act and to make related and consequential amendments to other Acts. (2009). 1st Reading February 2, 2022, 44th Parliament, 1 session. https://www.parl.ca/legisinfo/en/bill/44-1/c-11https://www.parl.ca/legisinfo/en/bill/44-1/c-11

Brill, Julie. (2011). The Intersection of Consumer Protection and Competition in the New World of Privacy. *Competition Policy International.* 7 (1),7-23. https://www.ftc.gov/sites/default/files/documents/public_statements/intersection-consumer-protection-and-competition-new-world-privacy/110519cpi.pdf

Campbell et al v *AG BC/AG Cda & Nisga'a Nation et al*, 2000 BCSC 1123. https://canlii.ca/t/1fmw9https://canlii.ca/t/1fmw9

Canada Labour Code. (RSC, 1985, c L-2), s. 2. https://laws-lois.justice.gc.ca/eng/acts/L-2/https://laws-lois.justice.gc.ca/eng/acts/L-2/

Chander, A.; Abraham, M.; Chandy, S.; Fang, Y.; Park, D.; Yu, I. (2021) Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation. *Policy Research Working Paper; No. 9594*. World Bank, Washington, DC. https://openknowledge.worldbank.org/handle/10986/35306https://openknowledge.worldbank.org/handle/10986/35306.

The Constitution Acts 1867 to 1982 (30 & 31 Victoria, c. 3 (U.K.)) https://laws-lois.justice.gc.ca/eng/const/page-1.htmlhttps://laws-lois.justice.gc.ca/eng/const/page-1.html.

Daginis, S. & Dillon, P. (October 2021) Privacy laws in Canada: to infinite fees and beyond. *Siskinds*. https://www.siskinds.com/privacy-laws-in-canada-to-infinite-fees-and-beyond/https://www.siskinds.com/privacy-laws-in-canada-to-infinite-fees-and-beyond/

Department of Justice Canada. (2020). *Modernizing Canada's Privacy Act: Online Consultation* https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/opc-cpl.htmlhttps://www.justice.gc.ca/eng/csj-sjc/pa-lprp/opc-cpl.html

Fdal, Omar Ali, 2021, "How to manage re-identification risks with synthetic data", Statice, Germany. https://www.statice.ai/post/how-manage-reidentification-risks-personal-data-synthetic-data

Fishing Lake First Nation v Paley, 2005 FC 1448 (CanLII).

First Nations Information Governance Centre. (2020). *A First Nations Data Governance Strategy: A Response to Direction Received from First Nations Leadership, Funded through Federal Budget 2018 in Support of the New Fiscal Relationship.* https://fnigc.ca/wp-content/uploads/2020/09/FNIGC_FNDGS_report_EN_FINAL.pdf.

First Nations Information Governance Centre. (2022) The First Nations Principles of OCAP® (Brochure). https://fnigc.ca/online-library/?wpv-publication-topic%5B%5D=ocap&wpv_aux_current_post_id=409&wpv_aux_parent_post_id=409&wpv_view_count=516.

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F. 31. https://www.ontario.ca/laws/statute/90f31https://www.ontario.ca/laws/statute/90f31

Gee, K. (2019). Introduction to Indigenous Canadian Conceptions of Privacy: A Legal Primer. *The Canadian Bar Association.* https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2019/Runner-up-of-2019-Privacy-and-Access-Law-Student-E#_ednref53%3E

Government of British Columbia. (2022). *Declaration Act Action Plan 2022-2027*. https://www2.gov.bc.ca/gov/content/governments/indigenous-people/new-relationship/united-nations-declaration-on-the-rights-of-indigenous-peoples/implementation
https://fnigc.ca/wp-content/uploads/2020/09/FNIGC_FNDGS_report_EN_FINAL.pdf

Government of Canada. (2022). *Figure 1: Industries under Federal Jurisdiction*. https://www.canada.ca/en/employment-social-development/corporate/reports/labour-transition-binders/minister-labour-2021/industries-infographic.html

Government of Canada. (2022). "The Government of Canada appeals the Quebec Court of Appeal's opinion on the Act respecting First Nations, Inuit and Metis children, youth and families." https://www.canada.ca/en/indigenous-services-canada/news/2022/03/the-government-of-canada-appeals-the-quebec-court-of-appeals-opinion-on-the-act-respecting-first-nations-inuit-and-metis-children-youth-and-families.html

Innovation, Science and Economic Development. (2019). Canada's Digital Charter in Action: A Plan by Canadians, for Canadians. https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/canadas-digital-and-data-strategy

Gordon v Canada (Health), 2008 FC 258. https://ca.vlex.com/vid/gordon-v-can-680872857https://ca.vlex.com/vid/gordon-v-can-680872857

Information and Privacy Commissioner of Ontario. (2016) *De-identification Guidelines for Structured Data*. https://www.ipc.on.ca/resource/de-identification-guidelines-for-structured-data/.

Johnson v Bell Canada, 1086 Federal Court of Canada (2008). https://ca.vlex.com/vid/johnson-v-bell-can-681362569https://ca.vlex.com/vid/johnson-v-bell-can-681362569.

Kardash, A. (2021). *Exploring the Compliance Cost and Impact of Canadian Federal and Provincial Privacy Legislative Reform*. Osler, Hoskin & Harcourt LLP. https://www.osler.com/en/resources/regulations/2022/exploring-the-compliance-cost-and-impact-of-canadian-federal-and-provincial-privacy-legislative-refo

Kukutai, T. & Taylor, J. (Eds). (2016). *Indigenous Data Sovereignty: Toward and Agenda.* Australian National University Press.

Mamalilikulla First Nation. (2020). *Privacy Policy*. https://mamalilikulla.ca/privacy-policy/https://mamalilikulla.ca/privacy-policy/

McKinsey & Company. (2022). Localization of data privacy regulations creates competitive opportunities. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities.

McQuinn, A. & Castro, D., 2019, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law", Information Technology and Innovation Foundation, https://openknowledge.worldbank.org/handle/10986/35306 https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law/

Nikolov, A., and Papernot, N. (2021). *To guarantee privacy, focus on the algorithms and not the data.* Schwartz Reisman Institute for Technology and Society. https://srinstitute.utoronto.ca/news/nikolov-papernot-privacy-bill-c11. https://srinstitute.utoronto.ca/news?author=60006430df80a433129c402a

NIL/TU,O Child and Family Services Society v. *B.C. Government and Service Employees' Union* [2010] 2 SCR 696. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7888/index.do

Office of the Information Privacy Commissioner for British Columbia. (2020). Order F20-57. https://www.oipc.bc.ca/orders/3494https://www.oipc.bc.ca/orders/3494 https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html

Office of the Privacy Commissioner of Canada. (2005). *Internet posting violates PIPEDA.* (PIPEDA Case Summary #2005-305). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/pipeda-2005-305/

Office of the Privacy Commissioner of Canada. (2008). *Organizations' Guide to Complaint Investigations under the Personal Information Protection and Electronic Documents Act. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/02_05_d_20/*

Office of the Privacy Commissioner of Canada. (2009). *Report of Findings into the Complaint Filed by the Canadian Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act by Elizabeth Denham Assistant Privacy Commissioner of Canada.* (PIPEDA Report of Findings #2009-008). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/#summary

Office of the Privacy Commissioner of Canada. (2010). *Manager's remark reveal's employee's salary - consent was necessary despite existing public disclosure requirement.* (PIPEDA Case Summary #2010-004). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2010/pipeda-2010-004/

Office of the Privacy Commissioner of Canada, 2012, *Privacy Issues on Reserve: Applicable Law and Unique Context*, Remarks of Chantal Bernier, Assistant Privacy Commissioner of Canada, at the 2011 Canadian Aboriginal Law Conference, https://www.priv.gc.ca/en/opc-news/speeches/2011/sp-d_20111125_cb/

Office of the Privacy Commissioner of Canada. (2013). *Interpretation Bulletin: Personal Information*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/

Office of the Privacy Commissioner of Canada. (2015). *Appendix 3 - Investigation Process*. Annual Report to Parliament 2014 on the *Personal Information Protection and Electronic Documents Act*. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201415/2014_pipeda/#heading-0-0-0-8

Office of the Privacy Commissioner of Canada. (2016). *First Nation develops a privacy policy following allegations of lost doctor's notes*. (Early resolution case summary #2016-03). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/ser/2016/er_03_160506/

Office of the Privacy Commissioner of Canada. (2017a). *Enforcement of PIPEDA*. https://www.priv.gc.ca/biens-assets/compliance-framework/en/index

Office of the Privacy Commissioner of Canada. (2017b). *Interpretation Bulletin: Commercial Activity*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/

Office of the Privacy Commissioner of Canada. (2019a). *PIPEDA in Brief*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

https://laws-lois.justice.gc.ca/eng/const/page-1.html

Office of the Privacy Commissioner. (2019b). *The Privacy Act in Brief*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/

Office of the Privacy Commissioner of Canada. (2020). *Privacy in a Pandemic*. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201920/ar_201920#heading-0-0-5.

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.htmlhttps://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html

Personal Health Information Protection Act (2004, S.O. c. 3, Sched. A). https://www.ontario.ca/laws/statute/04p03https://www.ontario.ca/laws/statute/04p03

Personal Information Protection Act (SBC 2003). https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01

Personal Information Protection Act (SA 2003 c P-6.5). https://www.canlii.org/en/ab/laws/stat/sa-2003-c-p-6.5/latest/sa-2003-c-p-6.5.html.

Privacy Act (1985 c. P-21). https://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.html.

Ponemon Institute LLC. (2017). The True Cost of Compliance with Data Protection Regulations: Benchmark Study of Multinational Organizations. *Globalscape.* https://static.helpsystems.com/globalscape/pdfs/guides/gs-true-cost-of-compliance-data-protection-regulations-gd.pdf

Pricewaterhouse Coopers LLC. (2021). Building data trust: Canadian Consumer Privacy Protection Act (CPAA) impact and readiness survey. https://www.pwc.com/ca/en/cybersecurity-and-privacy/publications/cppa-readiness-survey-en.pdf

Reference re Subsection 18.3(1) of the Federal Courts Act, 2021 FC 723. https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/499997/index.do

Reference to the Court of appeal of Quebec in relation with the Act respecting First Nations, Inuit and Metis children, youth and families, 2022 (C.A. Qc). https://courdappelduquebec.ca/en/judgments/details/reference-to-the-court-of-appeal-of-quebec-in-relation-with-the-act-respecting-first-nations-inuit/

Rodgers v Calvert, 2004 CanLII 22082 (ON SC). https://www.canlii.org/en/on/onsc/doc/2004/2004canlii22082/2004canlii22082.html

Sia Partners. (December 2017). *GDPR compliance to cost FTSE100 firms $15 million, banks face largest bill.* https://www.consultancy.uk/news/15101/gdpr-compliance-to-cost-ftse100-firms-15-million-banks-face-largest-bill

Sga'nism Sim'augit (Chief Mountain) v Canada (Attorney General), 2013 BCCA 49. https://canlii.ca/t/fw02jhttps://canlii.ca/t/fw02j

Snipp, Matthew. (2016) "What does data sovereignty imply: what does it look like?", in Taylor J, Kukutai T. editors, Indigenous Data Sovereignty: Toward an Agenda. https://press-files.anu.edu.au/downloads/press/n2140/pdf/book.pdf

State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada, 2010 FC 736. http://www.canlii.org/en/ca/fct/doc/2010/2010fc736/2010fc736.htmlhttp://www.canlii.org/en/ca/fct/doc/2010/2010fc736/2010fc736.html

Taufick, Roberto D. (2021). "The underdeterrence, underperformance response to privacy, data protection laws", *Technology in Society.* Oxford Vol. 67. https://doi.org/10.1016/j.techsoc.2021.101752

Tla'Amin First Nation. (2016). *Freedom of Information and Protection of Privacy Act*. https://www.tlaaminnation.com/wp-content/uploads/2016/11/Freedom-of-Information-Protection-Privacy-Law.pdf.

Tsawwassen First Nation. (2009). *Freedom of Information and Protection of Privacy Act.* http://www.tsawwassenfirstnation.com/pdfs/TFN-Laws-Regulations-Policies/Laws/Laws/FOIPOP_Act_2009.pdf

UN General Assembly (2007). *United Nations Declaration on the Rights of Indigenous Peoples.* https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdfhttps://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf

United Nations Declaration on the Rights of Indigenous Peoples Act, S.C. 2021, c. 14. https://laws-lois.justice.gc.ca/eng/acts/U-2.2/page-1.htmlhttps://laws-lois.justice.gc.ca/eng/acts/U-2.2/page-1.html

Westbank First Nation (2018) *Westbank First Nation Freedom of Information and Protection of Privacy.* https://www.wfn.ca/docs/freedom_of_information_and_protection_of_privacy_laaw_final.pdf.

Williams, J., Vis-Dunbar, M., Weber, J. (2011). First Nations Privacy and Modern Health Care Delivery. Indigenous Law Journal 10 (1), 101-132. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1736844

Witty v Mississauga First Nation, 2021 FC 436.

Wyndowe v Rousseau, 2008 FCA 39. https://www.canlii.org/en/ca/fca/doc/2008/2008fca39/2008fca39.html

Mamalilikulla First Nation. (2020). *Privacy Policy*. https://mamalilikulla.ca/privacy-policy/

Westbank First Nation (2018) *Westbank First Nation Freedom of Information and Protection of Privacy.* https://www.wfn.ca/docs/freedom_of_information_and_protection_of_privacy_law_final.pdf

APPENDIX 1: EXCEPTIONS TO APPLICATION OF PIPEDA

PIPEDA Exceptions	Application	Sources
This part does not apply to: 4 (2) (a) any government institution to which the *Privacy Act* applies	The *Privacy Act* applies to federal **government institutions**, defined under s. 3 of the *Act* as: "a) any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule, and b) any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the *Financial Administration Act*"	Office of the Privacy Commissioner. (2019) *The Privacy Act in Brief.* https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/. *Privacy Act* (1985 c. P-21). https://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.htmlhttps://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.html. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/
This part does not apply to: 4 (2) (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose	"Personal information collected by an individual solely for the individual's personal reasons. If this information, exempt in the hands of the individual, is an e-mail sent or received at work, it would be contrary to the purposes of the Act if that same information, once stored on the organization's backup system, would then not also be exempt from production by the organization." [*Johnson* at para 32]	*Johnson v Bell Canada*, 1086 Federal Court of Canada (2008). https://ca.vlex.com/vid/johnson-v-bell-can-681362569.

PIPEDA Exceptions	Application	Sources
This part does not apply to: 4 (2) (c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose	As of now the courts have only interpreted "journalistic purposes." The journalistic purposes aspect of this exception is meant to prevent PIPEDA from having a chilling effect on the freedom of the press. In 2017 the Federal Court ruled: "that an activity should qualify as journalism only where its purpose is to (1) inform the community on issues the community values, (2) it involves an element of original production, and (3) it involves a "self-conscious discipline calculated to provide an accurate and fair description of facts, opinion and debate at play within a situation". Those criteria appear to be a reasonable framework for defining the exception." (*A.T. v Globe24h.com* at para. 68)	Scassa, Teresa; Deturbide, Michael Eugene. *Electronic Commerce and Internet Law in Canada*. CCH Canadian Limited., 2004. *A.T. v Globe24h.com, 2017 FC 114*.
26 (2) The Governor in Council may, by order, **(b)** if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.	The privacy laws of Alberta (*Personal Information Protection Act)*, British Columbia (*Personal Information Protection Act*) and Quebec (*Act Respecting the Protection of Personal Information in the Private Sector*) "have been deemed substantially similar to PIPEDA". The health information laws of New Brunswick (*Personal Health Information Privacy and Access Act*), Newfoundland and Labrador (*Personal Health Information Act*), Nova Scotia (*Personal Health Information Act*), and Ontario (*Personal Health Information Protection Act*) are also deemed substantially similar to PIPEDA.	Office of the Privacy Commissioner of Canada. "Provincial laws that may apply instead of PIPEDA." (May 2020) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/ Office of the Privacy Commissioner of Canada. "*Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts*." (November 2004) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/

APPENDIX 2: COMPARISON OF PIPEDA AND CPPA

***PIPEDA* Provision**	***CPPA* Provision**
Definitions 2 (1) The definitions in this subsection apply in this Part. *personal information* means information about an identifiable individual.	Definitions 2 (1) The following definitions apply in this Act. *personal information* means information about an identifiable individual.
Limit (2) This Part does not apply to (a) any government institution to which the *Privacy Act* applies; (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or (c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.	Limit (4) This Act does not apply to (a) any government institution to which the *Privacy Act* applies; (b) any individual in respect of personal information that the individual collects, uses or discloses solely for personal or domestic purposes; (c) any organization in respect of personal information that the organization collects, uses or discloses solely for journalistic, artistic or literary purposes;
s. 5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.	s. 12(1): An organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances, whether or not consent is required under this Act.
7 (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if ...	15 (1) Unless this Act provides otherwise, an organization must obtain an individual's valid consent for the collection, use or disclosure of the individual's personal information.

***PIPEDA* Provision**	***CPPA* Provision**
7 (2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention; ...	Breach of agreement or contravention 40 (1) An organization may collect an individual's personal information without their knowledge or consent if it is reasonable to expect that the collection with their knowledge or consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of federal or provincial law. Contravention of law — initiative of organization 45 An organization may on its own initiative disclose an individual's personal information without their knowledge or consent to a government institution or a part of a government institution if the organization has reasonable grounds to believe that the information relates to a contravention of federal or provincial law or law of a foreign jurisdiction that has been, is being or is about to be committed.
7 (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if ... (d) the information is publicly available and is specified by the regulations; or ...	51 An organization may collect, use or disclose an individual's personal information without their knowledge or consent if the personal information is publicly available and is specified by the regulation**s.**
7(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if (c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;	35 An organization may disclose an individual's personal information without their knowledge or consent if (a) the disclosure is made for statistical purposes or for study or research purposes and those purposes cannot be achieved without disclosing the information; (b) it is impracticable to obtain consent; and (c) the organization informs the Commissioner of the disclosure before the information is disclosed.
7(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if (b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual.	30 An organization may use an individual's personal information without their knowledge or consent for the purpose of acting in respect of an emergency that threatens the life, health or security of any individual.

FNIGC | CGIPN

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

HEAD OFFICE
341 Island Road, Unit D
Akwesasne, ON K6H 5R7

OTTAWA OFFICE
180 Elgin Street, Suite 1200
Ottawa, ON K2P 2K3

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

fnigc.ca