



# LEGAL ASPECTS OF FIRST NATIONS INFORMATION GOVERNANCE

Prepared for the AFNIGC, OIPC and FNTN  
Privacy Education Series  
November 1, 2017

Krista Yao  
Barrister & Solicitor  
Nadjiwan Law Office  
[krista@nadjiwanlaw.ca](mailto:krista@nadjiwanlaw.ca)

# WHAT IS FIRST NATIONS INFORMATION?

Any information or data set that is capable of identifying:

- First Nation communities
- FN membership
- Indian status, or
- Residence on a reserve.

# WHO HOLDS FIRST NATIONS INFORMATION?

INAC

Health Canada

Statistics Canada

First Nation

Health Clinics

Schools

Provincial health and education systems

Social Service agencies

Service Providers

Universities – Researchers

Private entities

First Nation organizations

# WHY OCAP<sup>®</sup>?

Through governance of their own data, First Nations can:

- Protect personal privacy
- Protect community privacy
- Exercise sovereignty over their own information (control who can collect, use, disclose information)
  - ensuring that First Nations information is used to benefit First Nations and to minimize potential harm associated with use of First Nations information.

# HOW IS FIRST NATIONS INFORMATION VULNERABLE?

- ❖ Existing privacy laws and ‘western’ culture value only PERSONAL privacy and not privacy of GROUP information. Standard ‘template’ research agreements and contribution/funding agreements do not protect community information or Indigenous knowledge.
- ❖ Government and Academic culture/attitude regarding ownership of information and intellectual property interests.
- ❖ The federal *Access to Information Act* and some provincial equivalents **require** government Ministries and institutions to release aggregate First Nation information, upon request. Not Alberta.

# ALBERTA – FOIP (the “harm” clause)

## Disclosure harmful to intergovernmental relations

21(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

(a) harm relations between the Government of Alberta or its agencies and any of the following or their agencies:

(i) the Government of Canada or a province or territory of Canada,

(ii) a local government body,

(iii) an aboriginal organization that exercises government functions, including

(A) the council of a band as defined in the Indian Act (Canada), and

(B) an organization established to negotiate or implement, on behalf of aboriginal people, a treaty or land claim agreement with the Government of Canada,

(iv) the government of a foreign state, or

(v) an international organization of states,

or

(b) reveal information supplied, explicitly or implicitly, in confidence by a government, local government body or an organization listed in clause (a) or its agencies.

(2) The head of a public body may disclose information referred to in subsection (1)(a) only with the consent of the Minister in consultation with the Executive Council.

(3) The head of a public body may disclose information referred to in subsection (1)(b) only with the consent of the government, local government body or organization that supplies the information, or its agency.

(4) This section does not apply to information that has been in existence in a record for 15 years or more.

# LEGAL TOOLS TO ASSERT FN SOVEREIGNTY OVER FN INFORMATION:

AGREEMENTS – when the FN does not have possession of the FN information

POSSESSION – when the FN holds its own information

# AGREEMENTS

Some situations where a FN cannot hold its own data:

- A law requires it
- Mixed records
- Shared service
- Capacity issue

Agreements can be used by FNs to control the collection, use, disclosure and destruction of First Nations information.

Data Sharing Agreements, Data Governance Agreements, Information Sharing Agreements Data Stewardship Agreement



# AGREEMENTS: SOME IMPORTANT ELEMENTS

- Establish FN ownership and intellectual property rights
- FN rights to terminate the agreement and what happens to the FN information/data upon termination/expiry.
- Aggregate information is protected to the same standards as personal information
- Audit rights and reporting requirements
- Strictly define and limit how the information can be used, who has access
- Pre-approval or right of dissent in any writing/publication and attribution of credit for published works
- Trigger the FOIP harm clause and establish all information as “confidential”
- For electronic records – **look at reporting functions** and who has access!!! Plug leaks.

# LIMITATIONS TO AGREEMENTS AS A TOOL

## ❖ ATIP/FOIPOP legislation

❖ Misses the “Possession” aspect of OCAP®.

❖ Doesn't necessarily build FN capacity.

❖ FN parties must carefully examine/draft agreements, because they will not typically contain important provisions to assert FN governance over FN information.

# POSSESSION – FIRST NATION AS ITS OWN DATA STEWARD

First Nations Own

First Nations Control

First Nations Access

First Nations Possession

# FN DATA STEWARDSHIP: STEPS

## First Nation as Data Steward

Enact **privacy and access laws**/policies

Develop privacy and security infrastructure (policies, procedures, hardware, software, HR).

Education - leadership, administration and community

## First Nation-controlled entities

Incorporate

Develop privacy and security infrastructure (policies, procedures, hardware, software, HR)

Education

Agreements with FN communities and outside entities

# SUMMARY

Consider where First Nations information is, how vulnerable it is to public disclosure and how FNs can exercise control over the information.

## Minimize vulnerabilities:

- Re-patriate the data to First Nation data stewards where possible.
- Where the FN cannot be steward of their own data – ensure that there are agreements in place that address FN concerns regarding Ownership, Control, Access and Possession.
- Be mindful of the impact of ATIP/FOIP legislation

Importance of education and building capacity in our communities.