



April 2014

Barriers and Levers for the Implementation of OCAP™

* First Nations Information Governance Centre
bmackay@fnigc.ca

Recommended Citation

First Nations Information Governance Centre, *. (2014). Barriers and Levers for the Implementation of OCAP™. *The International Indigenous Policy Journal*, 5(2).

DOI: 10.18584/iipj.2014.5.2.3

Barriers and Levers for the Implementation of OCAP™

Abstract

This article discusses the obstacles to and supports for the implementation of the First Nations Principles of OCAP™, specifically in the context of data holdings within Aboriginal Affairs and Northern Development Canada (AANDC) and the Government of Canada. It cites three types of barriers (legal, knowledge and capacity, and institutional) that obstruct OCAP™ and examines how federal legislation such as the *Privacy Act* and *Access to Information Act* undermine these First Nations Principles. It continues by exploring supports available to help operationalize OCAP™, including legal, policy, knowledge and capacity-based levers. It concludes by outlining how AANDC's increased knowledge about OCAP™ could help support capacity building in First Nations communities.

Keywords

OCAP, First Nations, governance, data, information, stewardship, privacy, FNIGC

Acknowledgments

Krista Yao (Nadjiwan Law), Contributor

Creative Commons License



This work is licensed under a [Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Barriers and Levers for the Implementation of OCAP™

Since its creation in 1998, the First Nations Principles OCAP™ have become the *de facto* ethical standard not only for conducting research using First Nations data, but also for the collection and management of First Nations information in general.¹

A set of principles that lay out the ground rules for how First Nations data can and should be used, OCAP™ (which stands for ownership, control, access and possession) provides guidance to communities about why, how, and by whom their information is collected, used, or shared. OCAP™ reflects First Nation commitments to use and share information in a way that brings benefit to the community, while minimizing harm. Through the elements of ownership, control, access, and possession First Nations are able to express their values related to community privacy and information governance.

OCAP™ was created by the First Nations Information Governance Centre (FNIGC) to help guide the development of the *First Nations Regional Health Survey* (FNRHS), the only First Nations-governed, national health survey in Canada that collects information about First Nation on-reserve and northern communities (First Nations Information Governance Centre, 2013). While the FNRHS is the leading example of how OCAP™ can be operationalized, there are many other examples in First Nations across Canada including: eHealth record systems, research agreements, health surveillance, and FNIGC's new survey initiative, the First Nations Regional Early Childhood, Education and Employment Survey (FNREEES) (First Nations Information Governance Centre, 2013a).

This article is intended as a discussion of the specific barriers and levers for the management and governance of First Nations information or data generally, and specifically, in the context of shared data systems within Aboriginal Affairs and Northern Development Canada (AANDC) and the Government of Canada. It is not intended as an attempt to define OCAP™ or to discuss OCAP™ criteria.²

Barriers

Legal Barriers

Identifying applicable laws. First Nations data should be governed in a manner that respects personal privacy as well as community privacy and First Nations information governance principles (OCAP™). Therefore, one of the first questions that must be answered when looking at any collection of First Nations data is to identify what legislation applies in what context.

First Nations must be satisfied that there are appropriate protections for their personal privacy. Where that is lacking, as a result of gaps in legislation or policy, then other tools must be used to fill these gaps. First Nations must also be satisfied that there is appropriate protection for community privacy. Since the

¹ Throughout this article, the term “First Nations data” and “First Nations information” is intended to describe data about First Nations, regardless of who has collected or who controls the data.

² For more information about OCAP™ its creation or its implementation, please visit FNIGC's section on OCAP™ on its website at <http://www.fnigc.ca/ocap>

concept of community privacy is not recognized in federal legislation, other tools and strategies must be utilized to apply OCAP™.

Because of the federal Crown's relationship with, and responsibilities to First Nations, Canada collects and holds more information on First Nations people than perhaps any other group in Canada. AANDC alone holds 210 data banks of First Nations data (Government of Canada, 2013). The collection, use, and disclosure of this information is regulated by the *Privacy Act* (Government of Canada, 1985b), the *Access to Information Act* (Government of Canada, 1985a), and the *Library and Archives of Canada Act* (LACA), all of which apply exclusively to federal government institutions (see Banks & Hébert, 2004). While the *Privacy Act* protects personal information, the *Access to Information Act* and the *Library and Archives of Canada Act* present legislative obstacles to OCAP™ that are discussed below.

Most often, AANDC collects information about First Nations and their members through the First Nation itself. However, none of the above three statutes apply to First Nations. In some cases First Nations may have their own privacy policies or laws. It is also possible that provincial or territorial legislation may apply to certain data holdings, such as personal health information. However, very often there is an absence of privacy regulation in First Nation communities, both from the perspective of personal privacy as well as community privacy and OCAP™ considerations. This gap can limit the capacity of First Nations to exercise effective governance over their own data.

Legislative obstacles. One of the most important principles within OCAP™ is that First Nations control the use and disclosure of First Nations data. In other words, information (records, reports, data) that identifies any particular First Nation or group of First Nations should not be used or disclosed without consent of the affected First Nation – regardless of where that information or data is held.

Unfortunately, this principle is defeated by Canada's *Access to Information Act*: federal legislation passed in 1985 provides public access to government information via an Access to Information and Privacy (ATIP) request (Government of Canada 1985a). ATIP legislation recognizes and allows the federal government to withhold from disclosure certain broad categories of information, such as:

- Information obtained in confidence from another government,
- Information injurious to the conduct of Canada in federal-provincial affairs,
- Information that is part of ongoing law enforcement investigations,
- Information that could be injurious to economic interests of Canada,
- Personal information, and
- Third party information, if it contains trade secrets, confidential financial, or commercial information (Government of Canada, 1985a).

ATIP goes on to define “government” for the purposes of the first bulleted exception to include any level of government from municipality to the United Nations and all of their organizations. However, the only First Nations that are recognized as governments are those that have entered into self-government

agreements or “modern treaties” with Canada, and “participating First Nations” under the *First Nations Jurisdiction over Education in British Columbia Act* (2006). That leaves an overwhelming majority of First Nations in Canada that are not recognized as “governments” for the purpose of engaging in confidential sharing of information with Canada.³

For these First Nations, all information that is shared or provided, or that is collected from their members is available for release upon public request unless it falls under one of the exception categories described above. While these exceptions may protect the personal privacy of First Nation members, it would not protect aggregate reports or demographic or survey data, nor would it protect any traditional knowledge, or reporting under contribution agreements. In fact, except for those few First Nations that the Act recognizes as “governments”, almost any information or data that First Nations provide to Canada or that Canada collects from its members and other sources (as long as names and personal identifiers are removed) can be released to the public under the *Access to Information Act*.

This means that federal databases such as the Non-Insured Health Benefits (NIHB) program, nominal rolls (education) data, financial reporting, and social services data are available upon request by Canadian residents provided personally identifying information is stripped. As a result of the *Access to Information Act*, AANDC and other federal government institutions cannot withhold disclosure of a significant amount of First Nations information within their control. This is particularly true with the digitization of data, allowing records to be easily stripped of personally identifying information and then released to the requesting public.

This vulnerability is demonstrated through Health Canada’s release of NIHB data to Brogan Inc., a health marketing and consulting company that was acquired in 2010 by global conglomerate IMS Health (Dumas & Chapman, 2010). Health Canada’s position was that de-identified NIHB data was available anyway under ATIP; accordingly, the data is released to Brogan (now IMS Health) to be sold for global pharmaceutical marketing and sales purposes.

As long as personally identifying information is capable of being digitally “stripped” it appears to be the federal government’s position that the remainder of the data is subject to disclosure under ATIP.

Canada’s Infosource regarding AANDC data holdings lists over 200 categories of records that are held by the department.

Just a sampling of the categories includes:

- Band Governance Management System containing information on First Nation by-laws, elections, estates, appeals, custom codes;
- Elementary and secondary data nominal roll;

³The situation is similar with most of the provincial and territorial equivalents to the *Access to Information Act*. However, Nova Scotia and Alberta recognize First Nation governments as “governments” with the capacity to share confidential information without being subject to disclosure pursuant to an ATIP request. Sharing data with these provinces is, therefore, much more manageable as community identifying information can be protected.

- First Nations and Inuit Youth Employment Strategy participant information;
- Post-secondary education data;
- Income assistance;
- Pre-employment and income support,
- First Nation Child and Family Services;
- The Indian Registry System (IRS) containing detailed personal and biographic information about all First Nation members. (Government of Canada, 2013)

All of these databases can be stripped of personal identifiers and mined for any purpose through an ATIP request. This is entirely inconsistent with OCAP™ principles because the remaining data still identifies individuals as First Nations people and it still identifies First Nation membership.

The legislative conflict with OCAP™ principles is further exacerbated through the *Library and Archives of Canada Act*, which mandates that all records (including electronic) in the control of federal departments or institutions be transferred to the Archives when they are no longer used by the department or institution (Banks & Hébert, 2004). Once transferred to the Archives, even personal information becomes vulnerable to an ATIP request because the *Privacy Act* does not protect the privacy of personal information if the person has been dead for more than 20 years (Government of Canada, 1985b). This means that through ATIP and LACA, even personally identifying information about First Nations people can be released (20 years after death). Since the federal government collects so much information about First Nations, this exposes First Nations and First Nation families to significantly greater potential harm and continuing problems with OCAP™.

The combination of the *Access to Information Act* and LACA is the greatest barrier to the practical application of OCAP™ principles for data within the control of any federal government institution. All First Nations information collected through the multitude of federal programs and through reporting requirements with various departments is vulnerable to public release. No agreement or understanding amongst First Nations and any federal department can avoid the application of this legislation.

The legislation also applies to information acquired by the federal government through data sharing agreements and licenses to use wherein First Nations and First Nation organizations agree to share data tabulations and summaries with the federal government. Entities such as The First Nations Information Governance Centre (FNIGC) make significant efforts through the agreements to preserve ownership and other intellectual property rights, to limit use and access, and to obtain reporting and accountability for use and access. All are important applications of OCAP™. However, in recognition that the tabulations and summaries are subject to release pursuant to an ATIP request, as soon as they are within the control of the federal government, FNIGC strives to restrict the agreement to cover tabulations and summaries that are acceptable for public disclosure.

Unfortunately, First Nations do not have the ability to restrict the amount or type of information that AANDC collects via its normal operations and the databases described above. Data sharing agreements,

service agreements, and licenses to use can be effective only if it is a First Nation sharing with AANDC. When AANDC already holds the data, First Nations have no ability to restrict access, use, or disclosure.

Knowledge and Capacity Barriers

Lack of available information. Lack of knowledge or incorrectly assumed knowledge is often a preliminary barrier to understanding OCAP™ and then, logically, to implementing OCAP™ in the context of information management.

OCAP™ is not a four-criteria shopping list that researchers or other First Nations data stewards may check off according to their own standards. OCAP™ must be understood in the context of a particular First Nation or First Nations. It involves consideration of First Nations governance structures, values, history, and expectations. What may work for one community may not be appropriate for another; what is acceptable at a national level may not be acceptable at a regional or community level.

One of the challenges with knowledge barriers is that there is admittedly a lack of detailed or specific information as to: “What is OCAP?” and “How do we make something OCAP-compliant?” One of the reasons for this is that OCAP™ may mean something different for each First Nation. Yet, there are some very common standards.

Unreliable information. It is also important that the source of knowledge be verified, since there are many myths and misconceptions associated with OCAP™. For example, some believe that if a First Nation individual is conducting research or holding data that the project is necessarily OCAP™-compliant. Others believe that Research Ethics Board approval covers all ethical requirements for First Nations research. The Tri-Council Policy⁴ also adds to the confusion (Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, & Social Sciences and Humanities Research Council of Canada, 2010).

The lack of understanding or comprehension is not only an issue for government and university researchers: It is also present within First Nation communities. First Nations leadership have many priorities and concerns that they are faced with on a daily basis - concepts such as information governance and assertion of First Nations control over data can seem rather abstract when they are also dealing with issues such as clean drinking water and adequate housing. Yet, it is no reason for government to omit consideration for OCAP™ in these communities.

Capacity limitations. A lack of capacity at the First Nation level is a factor that stems from knowledge barriers as well as financial limitations. Many individual First Nation communities do not

⁴*The Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (Chapter 9 Research Involving the First Nations, Inuit and Métis Peoples of Canada) is generally seen as the ethical standard for academic research, yet it presents ways to avoid First Nations jurisdiction over First Nations data, and does not meet OCAP™ principles for First Nations information governance (Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, & Social Sciences and Humanities Research Council of Canada, 2010).

have the capacity⁵ to create their own information governance infrastructure, capable of securely holding a variety of First Nations' data (such as membership, health information, education information, housing, and social services). Yet, this data exists and can end up being held without a vigorous security and privacy framework within a First Nation or outside the First Nation by government or other service providers that are not necessarily accountable to First Nations for their stewardship and use of the data.

Institutional Barriers

In addition to legal and capacity issues, barriers to the application of OCAP™ principles arise on a very practical level from the culture of the organization that holds and uses information.

Academic culture. In universities, for example, there is an academic culture where researchers assume that they own the data that they collect and that they hold all intellectual property rights to the data. The competitive culture of academic research often prevents collaborative thinking and attribution of research credit to the subjects of that research. Assertions of First Nation control or ownership over research data often lead to accusations of stifling research or preventing an un-biased reporting of research results. This reaction is a reflection of a researcher's lack of knowledge or understanding about OCAP™, but it also represents an academic culture that can view research as a commodity and a source of prestige and academic advancement.

The biases and assumptions that arise from an academic culture can also be transferred to government when those same researchers become employed in the public service.

Administrative pressure. There are other practical and administrative barriers to the application of OCAP™ principles in the collection, management, and sharing of information. One such roadblock arises due to the rigidity of institutional or government legal or contract staff that refuse to or are unable to modify their "standard-form contracts" whether they are service agreements, contribution agreements, or otherwise. Many of these contracts have unreasonable and unwarranted demands regarding intellectual property, including the abandonment of moral rights and ownership of data. These requirements are inconsistent with OCAP™ and changes to the agreements typically do not impact upon the services provided or delivered under the agreement. Nonetheless, because of the bureaucracy involved in producing the template contracts and making amendments, there is often no ability to negotiate a more OCAP™-acceptable agreement.⁶

Time could also be considered an institutional barrier. It is very typical for funding (through contribution agreements or service agreements) to be significantly delayed. This often results in a "take-it-or-leave-it" proposition for First Nations, who are often pressured into signing contracts in a manner that is inconsistent with OCAP™ principles. First Nations are then pressured with the choice of either abandoning OCAP™ concerns so that funds can flow and commitments can be met, or abandoning important work due to OCAP™.

⁵ Capacity can include: the necessary policy and procedural framework, secure facilities, technical personnel, agreements, privacy training, and the necessary financial resources.

⁶As a matter of clarity, this section describes agreements wherein First Nations provide information or other records that they understand will be subject to release under ATIP. However, consistent with OCAP™, the First Nation would still retain ownership rights and moral rights in the product.

When dealing with contract amendments and time constraints, government employees working with First Nations also feel pressured and have proven to not only understand OCAP™ concerns but also be capable of advocating for the necessary changes. This leads to frustration at the level of government staff as well, as they try to navigate their own bureaucratic processes.

Levers

Legal and Policy Levers

Enacting legislation. First Nation laws are a tool that can help address some of the barriers associated with jurisdiction and capacity. A privacy law, with accompanying policies and procedures, would support a First Nation in holding its own data.

Specifically, after conducting a jurisdictional review on applicable legislation, a First Nation may find that there is no applicable privacy legislation. The absence of an enforceable privacy standard will impact upon the perception of privacy protection by First Nation members as well as by government partners. It is no surprise that the only First Nation that holds its own NIHB data and First Nations Health Institute System (FNHIS) data, the Mohawk Council of Akwesasne, is also one of the few First Nations that also has its own privacy law.

A First Nation's exercise of jurisdiction in the area of privacy protection also builds capacity within a community for privacy protection. Such a law can deal with both personal privacy and community privacy, incorporating universal standards of personal privacy together with OCAP™ principles. A First Nation privacy and security infrastructure can then be built in a manner that supports the law and a community's own values and principles regarding privacy.

Another tool that could be part of a privacy law, or be included as a separate piece, is a freedom of information or access to information law. This could be used by a First Nation to regulate how information about the First Nation and its members can be collected, used, and disclosed, again incorporating the community's own values and principles regarding OCAP™.

Avoiding ATIP. As described above, ATIP legislation is perhaps the most significant OCAP™ barrier associated with government control over First Nations data. The best lever in preventing this vulnerability is for the federal government to amend the *Access to Information Act* and the *Library and Archives of Canada Act*. Ideally, those amendments would see recognition of OCAP™ principles and mechanisms to allow First Nations to govern the collection, use and disclosure of the data within government control. More realistically, the federal government could follow the lead of provinces such as Alberta and Nova Scotia, and simply recognize First Nation governments as “governments” in the same manner as international, provincial, municipal, and other governments are already recognized. Such an amendment would permit First Nations to share confidential information with the federal government. Apart from these types of amendments, there are some ways to work around the problems that ATIP presents:

- **Records disposition authority:** The *Library and Archives of Canada Act* requires all records in government control to be sent to the National Archives, where they will eventually be made available to the public. To prevent the release of First Nation information that could

be harmful to First Nations, a records disposition authority (RDA) may be sought from the National Archivist, permitting destruction.

In practice, it seems to be very difficult to obtain an RDA that permits the destruction of First Nations data. However, it is authorized by statute and an RDA has been obtained by Health Canada for some First Nation health records.⁷

This work-around could be used to prevent the transfer of First Nations data to the Archives (including personal records) but it would be no help for records that are still held by a federal institution such as AANDC.

- **Limit Disclosure of First Nations Data:** Another strategy to avoid the unwanted disclosure of First Nations data under ATIP is for First Nations to only disclose data to Canada that they are prepared to have disclosed to the public in the event of an ATIP request. This option correctly assumes that all data is vulnerable to ATIP requests and therefore only releases data that First Nations have already determined will not cause undue harm if released to the public. This is the strategy adopted by First Nations in relation to the *First Nations Regional Health Survey*.

As indicated above, this strategy would only be available where the First Nation or First Nations organization already has stewardship over the relevant data, information or reports and is sharing with the federal government. Of course it would not apply for records already in government control.

- **Change the Data Steward:** The best and only reliable method of preventing application of ATIP is to prevent First Nations data from being within the control of a federal institution.

This can be done through:

- First Nations⁸ assuming stewardship of their own data; and
- Retaining a third-party data steward not subject to ATIP legislation.

The third party could be a university, a provincial partner, or a private corporation. However, a legislative review would still have to be conducted to ensure that there are no other barriers in relation to an alternative data steward. For example, if a province were considered as a data steward, the province's freedom of information legislation would have to be reviewed for similar barriers. In some provinces, colleges and universities also fall under provincial freedom of information legislation.

In either case where data stewardship is moved to a First Nation or to a third party, First Nations and Canada could govern the terms of access to and use of the data through a data-sharing agreement.

⁷Although that RDA was not entirely satisfactory because it left discretion with the Minister of Health whether or not personal health records would be submitted to the Archives.

⁸This could also include a First Nation organization, if that organization is directly accountable to First Nations in accordance with their practices and customs. Another government entity would not qualify because it would also be under ATIP.

Because Canada would not have control over the data, it would not be subject to release under an ATIP request, yet the data could be used for the intended purposes.

Ideally, in order to be consistent with OCAP™ principles of First Nation “possession,” First Nations or First Nation-controlled organizations must be the data steward. However, there are some situations where a third party data steward may be necessary. These situations would arise when the First Nation or First Nation-controlled organization does not have the necessary capacity. For example, the First Nation may not have the necessary security and privacy infrastructure; it may not have qualified personnel or equipment to perform data cleaning or other technical work on the data; or the data may contain personal health information that may be subject to provincial health information legislation with certain requirements or qualifications for health information custodians. As First Nations’ capacity in the area of information governance grows, the need for third-party data stewards would naturally decrease.

Knowledge and Capacity Levers

Creating an infrastructure that contains appropriate laws, policies, procedures, and agreements can address most of the legal barriers to the application of OCAP™. The remaining barriers can be overcome through sharing knowledge and building capacity. Some knowledge levers might include:

- Sharing knowledge about OCAP™ (background and application) with academics and government, helping to build a new culture for First Nations information; and
- Educating government legal and contracting staff about OCAP™, its requirements and how contracts may be amended to meet the needs and values of First Nations and government.

As discussed above, government staff that work closely with First Nations and information governance tend to have a very good understanding of First Nations concerns, OCAP™ principles and the rationale behind the changes that First Nations seek. If that level of understanding could migrate to all users of First Nation data and to legal and contract staff, many of the identified barriers within government could be alleviated.

In terms of building capacity for information governance within First Nations communities, some levers to consider include:

- Making OCAP™ tools available for use by communities, such as:
 - Suggested OCAP™ “standards” (i.e. how to preserve ownership and other intellectual property rights),
 - Data-sharing agreement templates,
 - First Nation privacy laws, and
 - Privacy and security policies and procedures for First Nations.

- Sharing OCAP™ knowledge with communities and leadership; and
- Assisting in the development of First Nation organizations as First Nations data stewards.

Conclusion

The limitations of the *Access to Information Act* will always be a primary concern for First Nations and a very strong motivation to limit federal government control over First Nations data. The reality is that due to the ATIP process most information First Nations share with AANDC and other federal departments and institutions is not confidential and cannot be protected. Limiting sharing and pushing for the transfer of First Nations data out of government control are the only viable strategies for avoiding an ATIP. There are many examples of how this has been effectively accomplished in a manner consistent with OCAP™ principles.

Other barriers are perhaps more easily confronted. Knowledge and capacity barriers together with institutional barriers can be minimized with education and resources. AANDC has already made significant efforts at increasing awareness and knowledge regarding the application of OCAP™. This has helped to build relationships and further important projects. The next step would seem to be ensuring that the knowledge disseminates to all relevant areas of the federal department, including administration, legal support and the ATIP office itself. This would help to promote changes to the culture and administration that is traditionally resistant to change.

AANDC could also take a role in facilitating the flow of resources to First Nation communities in order to develop knowledge and capacity for information governance. First Nations and First Nation organizations that have an infrastructure in place to ensure personal and community privacy will give AANDC more potential options in terms of data governance, including the identification of potential data stewards.

Thus, the building of knowledge and capacity can only assist AANDC in identifying suitable options for the stewardship of First Nations data in a manner that fulfills OCAP™ principles, while also meeting government requirements for the use and analysis of data, together with the protection of personal privacy.

References

- Banks, S., & Hébert, M. (2004). *Legislative summary: Bill C-8: The Library and Archives of Canada Act*. Retrieved from <http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/37/3/c8-e.pdf>
- Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, & Social Sciences and Humanities Research Council of Canada. (2010). Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans. Retrieved from http://www.pre.ethics.gc.ca/pdf/eng/tcps2/TCPS_2_FINAL_Web.pdf
- Dumas, A., & Chapman, M. (2010, July 3). *Data sharing agreement: First Nations Inuit Health Branch (FNIHB) and Brogan Consulting Inc.* (Resolution No.: 30/2010). Winnipeg (MB): Annual General Assembly (CAN).
- First Nations Information Governance Centre. (2013a). *About FNREES*. Retrieved from <http://www.fnigc.ca/our-work/fnrees/about-fnrees.html>
- First Nations Information Governance Centre. (2013b). *About RHS*. Retrieved from <http://www.fnigc.ca/our-work/regional-health-survey/about-rhs.html>
- First Nations Jurisdiction over Education in British Columbia Act (S.C. 2006, c. 10). Retrieved from <http://laws-lois.justice.gc.ca/eng/acts/F-11.75/page-1.html>
- Government of Canada. (R.S.C. 1985a). *Access to Information Act*, c. A-1, s. 13.
- Government of Canada. (2013). *Info Source: Sources of Federal Government and Employee Information*. Retrieved from Government of Canada, Info Source website: <http://www.aadncaandc.gc.ca/eng/1353081939455/1353082011520/>
- Government of Canada. (R.S.C. 1985b). *Privacy Act*, c. P-21, a. 3 “personal information” (m).