Information and Privacy Commissioner Comments on the *Access to Information and Protection of Privacy Act* (ATIPP Act) Review Report Issued by Government of Yukon in December 2016

BACKGROUND

The *Access to Information and Protection of Privacy Act* (ATIPP Act or Act) requires that a comprehensive review of the Act occur at least every six years. In December 2015, the Minister of Highways and Public Works (HPW), the department responsible for the ATIPP Act, announced that a review would occur in 2016 and 2017.

A public survey was conducted by HPW in the summer of 2016. In December 2016, the government released the *Access to Information and Protection of Privacy Act* Review Report (Report). The Report identifies that its purpose "is to provide an assessment of the current state of the ATIPP Act".[1] After reviewing the Report, I have several concerns about some of the comments appearing in the Report, particularly those pertaining to the privacy provisions of the ATIPP Act.

The intent of my comments about this Report is to help the public understand how the privacy provisions of the ATIPP Act operate, so that they can be more informed about their privacy rights under the existing Act and can properly assess whether the comments contained in the Report could result in legislative amendments that may negatively impact their privacy rights.

GENERAL COMMENTS

The ATIPP Act was brought into effect in Yukon 22 years ago, in 1995. The privacy provisions in the ATIPP Act are essentially the same as when the Act was proclaimed and are very similar to those in every public sector privacy law across Canada. The principles which guided the creation of the privacy provisions have not changed since 1995 and nor should they.

Privacy laws were established in Canada in the public sector first. These laws were designed for one purpose – to ensure individuals have control over their personal information when receiving publicly funded services.[2] Later, privacy laws were established for the private and health care

[1] Access to Information and Protection of Privacy (ATIPP) Act Review Report, December 2016, Yukon Department of Highways and Public Works, at p.2.

[2] The Supreme Court of Canada in *Alberta (Information an Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, stated in reference to the objective of privacy laws that "The focus is on providing an individual with some

sectors. These laws were also designed so that individuals could control their personal information in these sectors. It is important that people understand that privacy laws are about control, they are not about protecting individuals from harm as the Report indicates. Any amendments to privacy laws must be considered from the standpoint of individual control over personal information. To do otherwise ignores the central reason these laws exist.

SPECIFIC COMMENTS

Below, I have focused my response to the Report in six areas, each of which deals with a concern raised in the Report.

The privacy rules in the ATIPP Act are too challenging

The Report suggests in a number of places that Yukon government has experienced challenges with the current version of the ATIPP Act. More specifically, the Report indicates that the ATIPP Act is overly complex and that government staff don't understand it.[3]

The ATIPP Act is no more complex than any other piece of legislation. In fact, the ATIPP Act has only nine provisions that a public body must apply in order to meet its privacy obligations under the Act. This is significantly less than the privacy provisions in the new *Health Information Privacy and Management Act* (HIPMA) that every health care provider, both large and small, must comply with. HIPMA has over 40 sections, with the collection, use and disclosure provisions alone containing over 100 provisions.

ATIPP Act Privacy Provisions Overview

Collection Rules

A public body may ***only*** collect personal information if a law says it is allowed to, for law enforcement, or to operate a program or activity of a public body. Contrary to what is stated in the Report, a public body has no authority to collect personal information based on the consent of an individual. [4] The reason for this is simple. Individuals do not have the ability to refuse to provide personal information when engaging public services. There is no choice; either they hand over their personal information or be denied service. This reality calls into question whether consent in the public services context could ever be voluntary.

A public body must collect personal information directly from the individual and tell them the purpose of collection. This rule ensures individuals know which public bodies have their personal information, why they have it, and what it will be used or disclosed for.

There is a loss of control over personal information when an individual is unaware that their personal information is being collected. That is why the Act contains only a few circumstances that allow a public body to indirectly collect personal information without the individual's knowledge or consent. These circumstances are when a public body is authorized to disclose it to

measure of control over his or her personal information:" "The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of democracy", at para 19.

[3] *Ibid.* 1, at p.5.

[4] *Ibid.* 1, at p.12.

another public body, to determine suitability for an award or honour, or for a proceeding or law enforcement.

Use Rules

A public body may ***only*** use personal information it collects for the same purpose it was collected or a consistent purpose. It may also use the information with the individual's consent or if another public body was authorized to disclose it. There are limits on the extent that the personal information can be used. These restrictions on the use of personal information are to ensure an individual is aware of how their personal information will be used, with just one circumstance that may result in them being unaware.

Disclosure Rules

A public body may ***only*** disclose personal information in 11 circumstances. They must disclose an individual's personal information in response to the person's request for access to this information, subject to certain exceptions. A public body may also disclose personal information to another person or body if the individual consents, or without consent if the disclosure is for the purpose it was collected or a consistent purpose. In all these circumstances, an individual should know who their personal information is being disclosed to.

An individual may not know when a public body is disclosing personal information in the following circumstances:

- when a public body discloses personal information in response to a request for access to the information by another person, if the disclosure would not be an unreasonable invasion of the individual's privacy,
- when a law allows it or requires it,
- when an employee of the public body requires it to perform their duties,
- when it is disclosed to legal counsel or insurers for a civil proceeding,
- when it is disclosed for the purposes of collecting a debt or making a payment, or for the purposes of an audit, law enforcement, archives, to protect health and safety or notify next-of-kin about an injury to an individual, or research.

These circumstances are limited and specific to minimize the loss of individual control over personal information.

Additional Rules

A public body must ensure the personal information they collect is accurate and correct, or annotate it, if it is found to be incorrect. They must ensure they do not over collect or improperly use personal information and they must secure it against loss, alteration, and unauthorized access, disclosure or disposal. They must also retain personal information for one year if they use it to make a decision that directly affects an individual.

The reality is that the rules in the ATIPP Act for protecting privacy are not overly challenging. The main contributing cause of the challenges experienced by the Government of Yukon with the ATIPP Act has more to do with the lack of full implementation of the Act, rather than the Act

itself. As was recognized in the Report, only now, 22 years following the enactment of the law, are these public bodies developing privacy policy and procedures, and training their staff.[5]

Conclusion: The ATIPP Act as it is currently written is a sound piece of legislation that if implemented properly would do what it was intended to do, which is to enable individuals to exercise control over their personal information when engaging services delivered by Yukon government departments. Any proposed amendments to the ATIPP Act that could negatively impact individual control must be carefully considered and minimized as much as possible, to ensure that the privacy rights afforded to citizens are not eroded.

"Personal information" is defined too broadly in the ATIPP Act

The Supreme Court of Canada identified the foundational principle of informational privacy as follows.

> *"…all information about a person is in a fundamental way his own, for him to communicate or retain…as he sees fit…"*[6]

The Federal Court of Appeal considered the meaning of personal information in Canada's *Access to Information Act.* In this Act, the meaning of personal information is stated as "information about an identifiable individual that is recorded in any form." The Court stated the following about the breadth of the definition.

> *…the language of this section is "deliberately broad" and "entirely consistent with the great pains that have been taken to safeguard individual identity". Its intent seems to be to capture any information about a specific person…Such an interpretation accords with the plain language of the statute, its legislative history and the privileged, foundational position of privacy interests in our social and legal culture.*[7]

In the ATIPP Act, personal information is defined as "recorded information about an identifiable individual"[8] which is almost the same as the definition of personal information in Canada's *Access to Information Act*. It is also the same as or similar to the definition of personal information in every public sector privacy law in Canada.

Conclusion: Given the foregoing, it is unclear how the definition could be narrowed without negatively impacting an individual's right to informational privacy. If a public body collects recorded information about an identifiable individual, then the ATIPP Act should apply to the information so that the individual can exercise control over this information.

[5] *Ibid.*1*,* at p.5.
[6] *Ibid.* 2*,* at para. 21.
[7] Canada *(Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board) (F.C.A.)*, 2006 FCA 157, at para. 36.
[8] The complete definition includes examples of the kinds of information that qualify as personal information.

The silo approach taken by the ATIPP Act is problematic

The Report suggests that because each government department is defined as a public body in the ATIPP Act, this creates challenges for compliance. More specifically, the Report indicates that this approach makes it difficult for individuals who are seeking access to their own personal information to determine which public body has it and difficult for the records to be tracked when there are changes to the structure of departments. The Report also indicates that this approach contributes to inconsistent privacy and access to information management across Yukon government departments.

The ATIPP Act is designed to operate the same way that governments do - in separate departments, each with its own specific mandate and headed up by a deputy minister who reports to a Cabinet Minister. Every deputy minister in Canada who is responsible for a department or ministry is required to implement public sector privacy laws. As is the case with other departmental matters, the deputy minister is accountable for this, including the management of personal information. It is unclear to me why personal information, which is a departmental asset like every other asset, is thought of differently. It shouldn't be.

When changes occur to the structure of government, each department must ensure that the records are managed properly during transition. This includes records containing personal information. If records cannot be located during or following a transition, then poor information management is to blame, not the ATIPP Act.

There is nothing in the ATIPP Act preventing Yukon government departments from working collaboratively to develop consistent privacy and information management practices and, in fact, they are now doing this.[9]

In reference to the silo approach, the Report states the following:

> *The separation of Yukon government into public bodies ensures no one public servant is able to access the information holdings of every department. Beyond this, the separation of public bodies does not add greatly to privacy protection*.[10]

It also states that the ATIPP Act creates "barriers" within and between departments.[11]

I find these statements troubling.

All privacy laws in Canada including the ATIPP Act were developed from a set of privacy principles.[12] One of these principles, which goes to the heart of protecting the confidentiality of personal information, is the safeguarding principle that includes a requirement that personal information only be made accessible to an employee on a need-to-know-basis; that is, when the

[9] A Yukon government-wide policy was developed and implemented in October 2015 that establishes a centralized resource to assist all Yukon government departments in the management and protection of personal information in support of compliance with the ATIPP Act and the HIPMA.
[10] *Ibid.* 1*,* at p.6.
[11] *Ibid.*
[12] These principles are now embedded in the National Standard of Canada entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96 and are replicated in Schedule 1 of Canada's *Personal Information Protection and Electronic Documents Act.*

employee needs access to the information to do their job. If one person in government were to have access to all the personal information held by every government department, this would amount to a catastrophic breach of citizens' privacy. The separation of public bodies ***does*** add greatly to privacy protection for this very reason. As well, this separation upholds other privacy principles – identifying purposes and limiting collection.

These privacy principles taken together require that only the personal information that is necessary for a specified purpose be collected by a body which has a legitimate purpose for its collection. It is unclear to me how these principles would be upheld if all of Yukon government, which is made up of separate departments with separate and distinct mandates, were to have access to all personal information held by all departments. It would likely result in the collection of significantly more personal information by a specific service or program that is operating within a department, as all Yukon government departments would wish to weigh in on the personal information required for a government-wide collection purpose. Additionally, the information collected would likely be stored in a database that is accessible to a significantly greater number of government employees. One significantly negative possible outcome would be that this information could then be used for surveillance of citizens which could negatively impact on citizens' rights.[13]

If Yukon government public bodies were collapsed under the ATIPP Act into one single public body as appears to be a suggested remedy in the Report to the "barriers" presented by the ATIPP Act, several key privacy principles would be violated, and citizens' privacy and other rights would be at risk.

Conclusion: For the foregoing reasons, the ATIPP Act should continue to apply as it has, with each department being a separate public body.

The ATIPP Act prevents innovation because personal information cannot be shared

It was suggested in the Report that the Yukon government doesn't share personal information within or between public bodies because the ATIPP Act prevents this.[14] This is simply not the case. Yukon public bodies routinely share personal information.

The ATIPP Act facilitates the sharing of personal information by allowing a public body to share it within or between public bodies so long as the sharing is for the purpose the information was collected or a consistent purpose. The ATIPP Act also facilitates the sharing of personal information with an individual's consent. Yukon government public bodies rely on these provisions daily in support of the sharing that occurs. What they cannot do under the current ATIPP Act is to share personal information for a different purpose, such as to create a centralized

[13] David Lyon, Director of the Surveillance Studies Centre at Queen's University in Canada, holds the view that surveillance in today's modern society occurs in a number of ways including through computer assistance. He claims that "governments collect and manipulate personal information for both benign and repressive purposes" (David Lyon on The Culture of Surveillance, April 16, 2012, https://www.youtube.com/watch?v=sRRl9cpVHy0). He also claims that the key task of surveillance is for social sorting and that the evolution of computer information technology (CIT) has made it much easier for the sorting and classification to take place due to its efficiency, convenience and speed. (Surveillance as Social Sorting, David Lyon, September 21, 2007, https://www.youtube.com/watch?v=xtAa-f-1rTg.

[14] *Ibid.* 1, at pp. 12 and 29.

client registry where an individual's contact information can be maintained as a central repository for use by all Yukon government departments. Even with the consent of individuals, the ATIPP Act currently restricts them from sharing personal information in certain circumstances.

Like the Government of Yukon, every provincial and territorial government has grappled with the challenges presented by their privacy laws, as they move to innovate and provide services in different ways, including online.

This evolution of the government service delivery model, including the digitization of these services, has a number of benefits to citizens. These benefits support a need for increased sharing of personal information in certain circumstances. My ATIPP Review Comments issued in 2015 focus primarily on this issue. In those comments, I made a number of recommendations on how to amend the ATIPP Act to achieve the right balance between privacy protection and allowing more sharing of personal information between Yukon government public bodies. I highlighted that in British Columbia's *Freedom of Information and Protection of Privacy Act*, a government ministry (a public body) is allowed to share personal information with another government ministry (another public body) if the two operate a common or integrated program or activity. Before the sharing occurs, the public bodies are required to enter into an agreement demonstrating that they in fact have a common or integrated program or activity and they need to share personal information as part of it. They must also complete a privacy impact assessment and submit it to BC's Information and Privacy Commissioner for feedback. This is a sensible solution and one that I support to ensure there is rigor in the sharing process and proper oversight.

Conclusion: There are ways for the Government of Yukon to be innovative, without reducing the protection of privacy.

Individuals are unable to verify the use of their personal information and who has it

The Report suggests that the public cannot verify what their personal information is being used for and that it is accurate. It also suggests that "the public cannot hope to find all the personal information that government holds".[15]

The ATIPP Act requires that individuals be told why their personal information is being collected. An individual from whom a public body collects information should, therefore, be able to ascertain what it will be used or disclosed for.

The ATIPP Act places the onus on a public body to take all reasonable steps to ensure the information collected is accurate. This is not the individual's responsibility. There are a number of ways that public bodies can meet this requirement, including in the provision of online services.

[15] *Ibid.* 1, p.12.

Every public body is responsible for knowing what personal information it has and where it is located, so that it can be properly protected and provided to an individual on request. Every public body that is subject to privacy laws in Canada has this same requirement.

Conclusion: The majority of individuals know what services they engage in government and to whom they provide their personal information. Yukon government is not that large. It should not be a hopeless task, as is suggested by the Report, for an individual to locate their personal information after they provide it to a Yukon government public body.

The Public doesn't understand the ATIPP Act

It was suggested in the Report that the public doesn't understand the ATIPP Act.[16] This is likely due to a number of factors. It could be because public bodies are failing to properly inform them of the reason personal information is being collected or about how to access information. It could also be that the Information and Privacy Commissioner's Office has done a poor job of informing the public about the Act as it is authorized to do.[17]

Conclusion: It is not the ATIPP Act that is to blame for the public's lack of awareness about it. Instead, the Government of Yukon and the Office of the Information and Privacy Commissioner should seek ways to improve public education about the ATIPP Act.

CONCLUDING REMARKS

My overall assessment of the ATIPP Act is that it is a good piece of legislation and, if it were properly implemented by public bodies, they would be able to apply the law more easily and effectively and afford citizens the right to control their personal information.

In light of the new beneficial government services model, I support changes to the Act that allow more sharing of personal information within and between Yukon government public bodies, so long as the sharing is properly balanced with appropriate controls and oversight. To achieve this balance, the privacy provisions of the Act need only minor amendments. My recommendations on how to achieve this balance can be found in my ATIPP Act 2015 Review comments, which are located at www.ombudsman.yk.ca.

The ATIPP Act, unlike most other laws, affects every person, resident in the territory or not, who engages services from Yukon government public bodies. The survey conducted was responded to by a very small number of people, less than 1% of Yukon's population.[18] I acknowledge that it is challenging to get public participation on legislation reviews. However, we should not allow the views of a very small number of people to negatively influence our rights under a law that affects us all.

---

[16] *Ibid.* 1, pp. 5 and 21.

[17] The IPC recently requested a budget allocation in 2017/18 for an additional resource to focus on communications to the public and others on the ATIPP Act, the HIPMA, the *Ombudsman Act*, and the *Public Interest Disclosure of Wrongdoing Act*.

[18] 124 people completed the survey (See p.2 of the Report). Only 106 were from Yukon.

LEARN ABOUT THE ATIPP ACT

To help the public learn more about how the ATIPP Act operates and their rights under it, my Office is hosting two public information sessions where I will provide an overview of the privacy provisions of the ATIPP Act. My team will also be at these events to answer questions. Coffee, tea and cookies will be served. These events are as follows:

ATIPP Act Public Information Sessions

Friday, January 20, 2017 from 11:00 am to 12:30 pm at the Whitehorse Public Library in the conference room located just off the main entrance.

Monday, January 23, 2017 from 7:00 pm to 8:30 pm in the location noted above.

VOICE YOUR OPINION

The Department of Highways and Public Works (HPW) indicated in the Report that it plans to draft potential amendments to the ATIPP Act and seek public feedback. If you have concerns about the comments in the Report, I strongly encourage you to contact the ATIPP Office in HPW, your member of the Yukon Legislative Assembly, or my Office in order to share your concerns before the amendments are drafted.

If you have concerns about the comments in this document or want to learn more about the ATIPP Act, please contact my office as follows.

Office of the Information and Privacy Commissioner

Mailing address:	Suite 201, 211 Hawkins Street, Whitehorse, Yukon Y1A 1X3
Telephone number:	867-667-8468 or toll free in Yukon at 1-800-661-0408 ext. 8468
Fax number:	867-667-8469
Email address:	email@ombudsman.yk.ca