Yukon Information and Privacy Commissioner

Access to Information and Protection of Privacy Act

2015 Review

Information and Privacy Commissioner's Comments

This page has been intentionally left blank.

TABLE OF CONTENTS

GLOSSARY OF TERMS

"AB" means Alberta

"AB's FOIP Act" means AB's *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25

"ATIPP Act" means Yukon's *Access to Information and Protection of Privacy Act*, RSY 2002, c 1

"BC" means British Columbia

"BC's FIPPA" means BC's *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165

"Commissioners" means the Federal, Provincial and Territorial information and privacy commissioners and includes the Ombudsman in Manitoba

"Designation Regulation" means the *Designation of Public Bodies Regulation*, YOIC 2009/240

"EI" means electronic information

"HIPMA" means Yukon's *Health Information Privacy and Management Act*

"IPC" means Yukon's Information and Privacy Commissioner

"MB" means Manitoba

"MB's FIPPA" means MB's *Freedom of Information and Protection of Privacy Act, The*, CCSM c F175

"NB" means New Brunswick

"NB's RTIPPA" means NB's *Right to information and Protection of Privacy Act*, SNB 2009, c R-10.6

"NL" means Newfoundland and Labrador

"NL's ATIPPA" means NL's *Access to Information and Protection of Privacy Act*, 2015, SNL 2015, c A-1.2

"NL's ATIPPA Review Committee" means the Committee comprised of Clyde K. Wells, Doug Letto and Jennifer Stoddart who reviewed Newfoundland and Labrador's *Access to Information and Protection of Privacy Act*

"NL's ATIPPA Review Report" means the Report of the 2014 Statutory Review, Access to Information and Protection of Privacy Act, Newfoundland and Labrador, Volume II: Full Report issued in March of 2015

"NL's Public Bodies" means the Public Bodies subject to NL's ATIPPA

"NS" means Nova Scotia

"NS FOIPOP" means NS's *Freedom of Information and Protection of Privacy Act,* SNS 1993, c 5

"NU" means Nunavut

"NU ATIPP Act" means NU's *Access to Information and Protection of Privacy Act*, SNWT (Nu) 1994, c 20

"NWT" means Northwest Territories

"NWT ATIPP Act" means NWT's *Access to Information and Protection of Privacy Act*, SNWT 1994, c 20

"ON" means Ontario

"ON's FOIPPA" means ON's Freedom *of Information and Protection of Privacy Act*, RSO 1990, c F.31

"OIPC" means the office of Yukon's IPC

"PEI" means Prince Edward Island

"PEI's FOIPP Act" means PEI's *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01

"PIA" means privacy impact assessment

"Public Bodies" means public sector entities subject to access to information and protection of privacy laws in Canada

"Private Bodies" means private sector entities

"RM Regulations" means the *Records Management Regulations*, YOIC 1985/17

"SK" means Saskatchewan

"SK's FOIP" means SK's *Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01

"YG Public Bodies" means a department of Yukon Government

"Yukon Public Bodies" means public sector entities in Yukon that are subject to the ATIPP Act and includes YG Public Bodies

RECCOMMENDATIONS SUMMARY

The following recommendations can be found in the **Access, Privacy and Innovation** section of these comments beginning on page 13.

Recommendation #1

Consideration should be given to amending Part 3 of the ATIPP Act to expand the authority of Yukon Public Bodies to collect and disclose personal information to facilitate innovation. If applicable, consideration should also be amending the ATIPP Act to authorize the creation of a service provider in a YG Public Body to be responsible for centralized citizen services.

Recommendation #2

The duties of Yukon Public Bodies to protect personal information should be increased in the ATIPP Act. At minimum these duties should include:

- **a requirement that Yukon Public Bodies complete a PIA for any proposed enactment, system, use of technology, project, program or activity that involves personal information and submit them to the Office of the IPC (OIPC) for review and comment;**
- **a requirement that Yukon Public Bodies notify the OIPC at an early stage of any proposed enactment, system, use of technology, project, program or activity that involves personal information, and for which a PIA will be developed, before the enactment is drafted, system acquired, or program or activity plan is finalized and consider any comments made by the OIPC with respect thereto;**
- **a requirement that a PIA be completed for development of a centralized service provider and that the PIA be submitted to the OIPC for review and comment;**
- **prior to development of the centralized service provider, the OIPC is provided with the plan for centralized services before the plan is finalized and consider any comments the OIPC has about the plan;**
- **a requirement that Yukon Public Bodies enter into information sharing agreements when sharing personal information;**
- **a requirement that Yukon Public Bodies submit draft information sharing agreements to the OIPC for review and comment, or a requirement that the Minister responsible for the ATIPP Act works with the OIPC to develop an information sharing code of practice;**
- **a requirement that Yukon Public Bodies notify individuals about a breach of their privacy (theft, loss, or unauthorized access, disclosure or disposition of personal information) and submit a report about the breach to the OIPC for review and comment;**
- **a requirement that Yukon Public Bodies make information available to the public about information sharing agreements entered into, PIAs developed, and breaches of privacy.**

Recommendation #3

The ATIPP Act should require Yukon Public Bodies to develop and maintain a privacy management program consisting of:

- **the ability to demonstrate accountability for privacy management through executive management support, designation of a privacy officer, and development of a reporting structure in respect of the privacy officer's activities;**
- **a personal information inventory and program controls: privacy policies and procedures, use of risk management tools (PIAs, security threat risk assessments, and ISAs); employee training programs and tools, service provider management, and external communications to the public including: privacy policies and procedures; notices about collection, use and disclosure of personal information, and information about rights and how to exercise them; and**
- **an oversight and review plan to identify and address deficiencies in the program.**

Recommendation #4

The IPC should be given the following additional general powers under Part 4 of the ATIPP Act to:

- **conduct own motion investigations where the IPC has reason to believe a Yukon Public Body is not complying with the ATIPP Act;**
- **conduct audits to ensure Yukon Public Bodies are complying with their obligations under the ATIPP Act;**
- **comment on the implications to privacy in respect of data-linking; and**
- **comment on use of information technology in the collection, storage or transfer of personal information.**

Recommendation #5

The IPC should be given the power under Part 4 of the ATIPP Act to share personal information as necessary with other Commissioners offices for the purposes of conducting joint investigations or audits.

Recommendation #6

Consideration should be given to granting the IPC the power under Part 4 of the ATIPP Act to provide education to inform Yukon Public Bodies about their duties and give advice to a public body. These powers would be beneficial for promoting improved privacy management practices in Yukon Public Bodies.

Recommendation #7

The IPC should be given the power under Part 4 of the ATIPP Act to:

- **make any recommendations necessary to remedy any non-compliance with the ATIPP Act in respect of any power granted;**

- **publish investigation and review reports including recommendations made; and**
- **publish special reports in respect of any authority granted under the ATIPP Act.**

Recommendation #8

The powers granted to the IPC for reviews under section 53 of the ATIPP Act should be expanded so they apply to all the IPC's powers including the power to comment and audit.

Recommendation #9

The ATIPP Act should enable a binding order to be issued following an investigation, review or audit by the IPC where the IPC finds a Yukon Public Body to have contravened or is contravening the ATIPP Act, the Public Body refuses to comply with the IPC's recommendation to remedy the non-compliance, and the IPC is of the view that there is a significant risk to privacy as a result of the non-compliance.

Recommendation #10

The ATIPP Act should require Yukon Public Bodies to apply information management practices that include development of policies and procedures in support of the right to access information. At minimum these requirements should include:

- **a requirement that Yukon Public Bodies develop policies and procedures to ensure that:**
  - **deliberations and actions undertaken and any decisions made by an employee that relates to his or her employment responsibilities are documented;**
  - **recorded information that is stored outside the Public Body's information management system, including on any mobile electronic devices, that is not transitory is transferred to the Public Body's information management system within a specified period after creation of the record;**
  - **there are clear consequences for employees who fail to comply with the policies and procedures; and**
  - **before a decision is made to acquire technology on which information will be stored, the Public Body consider the impact on access to information rights and evaluate whether the benefits of using the technology outweigh removal of access to information rights, and that this decision and the reason for the decision are documented and retained for a specified period;**
- **a requirement that Yukon Public Bodies consult with the IPC during the development of information management policy and procedure**.

The following recommendation can be found in the **Rethinking the Role of the Records Manager** section of these comments beginning on page 44.

Recommendation #11
The responsibilities of the records manager in the ATIPP Act should be eliminated or significantly reduced.

The following recommendations can be found in the **Scope of the ATIPP Act** section of these comments beginning on page 51.

Recommendation #12
Yukon municipalities should be made subject to the ATIPP Act.

Recommendation #13

- **The boards, commissions, foundations, corporations or other similar agencies that are public bodies under the ATIPP Act should be specified in the Designation Regulation.**

The following recommendations can be found in the **Additional ATIPP Act Amendments** section of these comments beginning on page 54.

Recommendation #14
The ATIPP Act should be amended to ensure that:

- **ATIPP Coordinators in each Yukon Public Body are given sole delegated authority to handle requests for access to information;**
- **no officials in Yukon Public Bodies other than the ATIPP coordinator are involved in the request unless they are consulted for advice in connection with the matter or giving assistance in obtaining and locating the information; and**
- **the identity and type of requester remains anonymous until the final response is sent to the requester by the ATIPP coordinator, except for requests made for personal information or the requests where the identity of the requester is necessary to respond to the request.**

Recommendation #15
Consideration should be given to requiring that ATIPP Coordinators be positioned at least a management level within Yukon Public Bodies and be provided adequate training about how to interpret and apply the ATIPP Act to ensure the provisions under Part 2 of the ATIPP Act are properly applied.

Recommendation #16
A public interest override provision similar to that recommended by NL's ATIPPA Review Committee should be included Part 2 of the ATIPP Act.

Recommendation #17
Subsections 5 (4) and (5) of the ATIPP Act should be repealed.

Recommendation #18

Consideration should be given to implementing a policy or process that requires Yukon Public Bodies to change the manner in which ministerial briefing records are assembled so that policy advice, recommendations and other Cabinet confidences are easily separable from factual information.

Recommendation #19

Section 69 of the ATIPP Act should be amended to include a requirement that any provisions in a Yukon law that is paramount over the provisions in the ATIPP Act are reviewed each six years during the comprehensive review of the ATIPP Act to evaluate whether these paramountcies are necessary.

Recommendation #20

Section 1 of the ATIPP Act should be evaluated to ensure the purposes are still accurately reflected given the shift from paper to electronic information management and greater emphasis on accountability.

Recommendation #21

The IPC should be granted authority in Part 4 of the ATIPP Act to require production of records relating to disputes about whether a request for access to records involves those records described in paragraphs 2 (1)(d), (e) and (g) of the ATIPP Act.

Recommendation #22

The terms "applicant", "complaint", "review", "request" and "third party" should be defined in section 3 of the ATIPP Act. See NL's ATIPPA for wording.

Recommendation #23

The relationship of the ATIPP Act with the HIPMA should be specified in section 4 of the ATIPP Act.

Recommendation #24

Paragraph 16 (1)(b) in the ATIPP Act should be repealed.

Recommendation #25

The term "published" in section 23 of the ATIPP Act should be defined.

Recommendation #26

Consideration should be given to developing a process to guide ATIPP Coordinators on the application of section 26 to reduce delays in providing access to information caused by unnecessary third party notifications.

Recommendation #27

Section 26 of the ATIPP Act should be repealed and a new section 11.1 added following section 11 that is similar to the third party notification provisions in section 19 of NL's ATIPPA.

Recommendation #28

Timelines to process a request for correction should be included in the ATIPP Act.

Recommendation #29

Section 34 of the ATIPP Act should be amended to add a requirement that upon receipt by a Yukon Public Body of a request for personal information or to correct personal information from an individual, the Public Body must retain the information for as long as necessary to allow the individual to exhaust any recourse under the ATIPP Act that he or she may have with respect to the request.

Recommendation #30

Section 36 of the ATIPP Act should authorize a Yukon Public Body to disclose personal information to an individual if the request is made by the individual for his or her own personal information.

Recommendation #31

The IPC should be authorized under Part 4 to discontinue an investigation or review in certain circumstances.

Recommendation #32

The IPC should be authorized under section 46 to delegate any duty or power under the ATIPP Act, including for conducting reviews.

Recommendation #33

Paragraph 54 (2)(a) of the ATIPP Act should be amended to place the burden of proof where personal information is at issue in a review on the public body to prove that the disclosure of the information would not be contrary to the ATIPP Act.

Recommendation #34

Section 67 of the ATIPP Act should be repealed and replaced with the following.

67 (1) A person who knowingly collects, uses or discloses personal information in contravention of this Act or the regulations is guilty of an offence and liable, on summary conviction, to a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.

(2) A person who knowingly

(a) attempts to gain or gains access to personal information in contravention of this Act or the regulations;

(b) makes a false statement to, or misleads or attempts to mislead the commissioner or another person performing duties or exercising powers under this Act;

(c) obstructs the commissioner or another person performing duties or exercising powers under this Act;

(d) destroys a record or erases information in a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records; or

(e) alters, falsifies or conceals a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records,

is guilty of an offence and liable, on summary conviction, to a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.

(3) A prosecution for an offence under this Act shall be commenced within 2 years of the date of the discovery of the offence.

Recommendation #35

Section 68 should be amended to authorize the Commissioner in Executive Council to make a regulation authorizing the waiving of fees to process a request for access to information if disclosure of the record is in the public interest.

ORIGINS OF ACCESS AND PRIVACY LAWS

In the early 1990's most jurisdictions in Canada recognized the importance of establishing the right of the public to access information held by public sector entities (Public Bodies) and the need to ensure that Public Bodies adequately protect the privacy of personal information. The right to access information is recognized as fundamental to the exercise of democracy and in this regard contributes to responsible government. The right to privacy has been recognized by Canada's highest court as having quasi-constitutional protection.[1]

In recognition of the importance of these rights, every jurisdiction in Canada has through the enactment of access and privacy laws established an oversight body responsible to ensure compliance. Access to information and privacy protection rights have been recognized on a global scale with nearly 100 jurisdictions in the world now having legislation in place to protect these rights.

In 1995, Yukon's Legislative Assembly passed the *Access to Information and Protection of Privacy Act* (ATIPP Act). With the passage of the ATIPP Act, Yukoners were guaranteed the right to access information held by Yukon's public sector entities (Yukon Public Bodies) subject to specific and limited exceptions. They were also guaranteed the right to have the privacy of their personal information held by Yukon Public Bodies protected in accordance with the requirements set out in the ATIPP Act. Yukoners were also guaranteed oversight protection by the Information and Privacy Commissioner (IPC) to ensure these rights are not infringed upon.

ACCESS, PRIVACY AND INNOVATION

Evolution of Public Bodies' Information Management

Most access and privacy laws in Canada have been in effect for twenty-plus years. How Public Bodies manage information has changed dramatically since these laws went into effect.

When most access and privacy laws came into effect, information within Public Bodies was primarily in paper form. Most communications were over the telephone or face to face. Email was a new technology used sporadically, and the use of electronic databases for information management was just emerging. Mobile devices, primarily cell phones, were not used to transmit information. Information sharing between Public Bodies was uncommon due to a more siloed service delivery approach.

Today, the use of information technology by Public Bodies to manage information is ubiquitous. Public Bodies' use of complex and integrated technology to manage information and the use of email

[1] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, [2013] 3 SCR 733, 2013 SCC 62 (CanLII), para. 19.

communications and mobile devices to transmit information is the norm. Sharing information between Public Bodies has increased exponentially as service delivery becomes more integrated and citizen focused.

Risks to Access and Privacy from Increased Use of Technology

Commissioners[2] across Canada who are charged with oversight responsibility for access and privacy laws over the years have, through their various reports and speeches, taken note of the increased use of information technologies by both Public Bodies and private sector bodies (Private Bodies) and have identified several areas of technological development that threaten access and privacy rights. Information about the key areas of technological development identified by the Commissioners and the risks to access and privacy associated with these developments are set out below.

1) The New Digital Economy

The advent of the Internet and cellular networks has increased the use of computers and mobile technology shifting the format of information from paper to digital. The digitization of information has led to a cultural shift in interaction with the information world. Individuals have a huge online presence and are constantly contributing to the mass of information available online. These individuals are beginning to expect access to services online, including those delivered by Public Bodies. This expectation and use of online services has increased awareness about how essential information is, including personal information, to developing the global and digital economy. Privacy protection is at risk due to the increased need for personal information to support the evolution of the digital economy.[3]

2) Big Data[4]

The massive amount of digital information being collected has led to the development of big data. The idea behind big data is that personal information about individuals can be shared and combined to

[2] Federal, provincial and territorial information and privacy commissioners (includes the Ombudsman in Manitoba).

[3] A recent article (Internet of Things and Cybersecurity, LaRoche, K.L. and Widdowson, S., Lexology, August 4, 2015) highlights the risks to privacy and security from this emerging field in the digital economy. In the article the authors note that: Internet of Things (IoT) is the development of web objects embedded with microchips capable of allowing sending and receiving data, and so connecting them to the Internet. IoT has a huge potential for business. A recent report predicts a potential economic impact of as much as 11.1 trillion per year by 2025 in nine specific settings – home automation and security, office security and energy, factory operations and optimization, retail, worksite operation and health and safety, human health and fitness, logistics and navigation, public health and transportation, and commercial vehicles. IoT poses huge privacy and security issues. Data and system security need to be at the forefront of any IoT Business Plan.

[4] "Big data" often refers simply to use of predictive analytics or other certain advanced methods to extract value from data, Wikipedia, https://en.wikipedia.org/wiki/Big_data, August 5, 2015.

create new personal information that is useable for specific purposes, such as marketing, or determining service needs, based on a profile created through the combined information.

Big data negatively impacts privacy rights of individuals because consumers lose control over the personal information when their personal information is combined from multiple sources to create new personal information. Big Data also creates security risks to privacy due to the ease at which the massive information repositories can be downloaded or transmitted and the multiple access points to the information.

Big data is valuable to governments as it facilitates better policy making and improves cost savings by combining information available.[5]

---

[5] In the Report of the 2014 Statutory Review, Access to Information and Protection of Privacy Act, Newfoundland and Labrador, Volume II: Full Report (NL's ATIPPA Review Report) issued in March of 2015, the Committee (NL's ATIPPA Review Committee), comprised of Clyde K. Wells, Doug Letto and Jennifer Stoddart, stated the following beginning on page 238:

> *Governments everywhere are attempting to make better policies and find savings by combining information available from their own internal sources—information gathered directly from individuals in the course of administering government programs such as income assistance, child protection, or health care—with other information available commercially.*
>
> *This information is purchased through commercial data brokers who aggregate and analyse personal information acquired by private corporations. Loyalty cards, draws, analyses of website visits and online browsing patterns, and registration for the provision of goods or services are all a rich source of data about people's consumer and financial habits, opinions, daily choices, and even travel itineraries.*
>
> *"Big data" is the term coined to describe the voluminous amount of information, much of it personal, being generated by the network of computers that assist in and document our daily activities. These activities range from driving a car to taking a jar off a supermarket shelf to visiting a bank machine to keeping a medical appointment. Many observers see in the analysis of big data great promise for future knowledge breakthroughs in vital areas such as health, agriculture, or accident prevention. The proponents of big data argue that analyzing available information with the appropriate algorithms should yield new trends, undocumented associations, and regular or irregular occurrences that have, until now, largely escaped attention.*
>
> *Carefully and appropriately used, big data can help us with many of the great challenges to the societies of the 21st century: environmental change, human health, and natural resource husbandry. But without the proper safeguards to prevent so much information revealing individual identities in embarrassing or harmful ways, the application of big data can lead to unplanned negative or discriminatory consequences to individuals. For example, using general characteristics of students who did not pursue higher education to justify the compulsory streaming of young people could result in the exclusion of able potential candidates, based on a generalization to which they are the exception. Personal freedom to achieve could be thwarted by machine-made decisions.*
>
> *In the future, citizens will increasingly be subject to decisions based on information they did not give to the government and did not know was shared with the government. Individuals and communities could be unaware they are being profiled. There has been extensive scholarship on this subject, particularly in the United States.*
>
> *Knowledge of information-related issues by the staff of the Commissioner's office could help government make wise decisions when it is confronted with policy and ethics challenges resulting from the aggregation of massive amounts of information about its citizens.*

3) Surveillance Technology

Use of surveillance is increasing. Surveillance is used for multiple purposes, some of which are not authorized.[6]

The nature of some technology results in unintended surveillance. For example, the use of smart meters allows the continuous collection of an individual's hydro information, providing the hydro company with information about when the individual is not home. Use of black boxes on cars provide insurers with information about a driver's activities behind the wheel for the purpose of identifying risks that inform insurance rates, but may be used by police to investigate the cause of an automobile accident or by insurers for determining fault. This information was not previously available. Use of surveillance in the workplace is also increasing along with the use of biometrics, such as facial recognition, as part of surveillance for identification purposes.

Surveillance technologies allow entities to collect information about who we are and our activities, sometimes without our knowledge, from information that was previously unquantifiable. Once this information is collected, it is unknown how it will be used and to whom it will be disclosed.

Access rights are also negatively impacted when surveillance is conducted using video or audio and the technology selected does not allow redaction of third party personal information from the video or audio record, even though this technology is available. As a result, individuals who have a right to access their own personal information are denied this right when their personal information cannot be separated from a record containing another person's personal information.

4) Mobile Devices

Increased use of mobile devices by Public Bodies' employees negatively impact access and privacy rights for a number of reasons.

The instant messaging feature on mobile devices is being used to conduct business. The information is not stored on institutional servers and there are, generally, no requirements that this information be transferred to these servers. There is no effective management of these messages and in most cases these messages are deleted a short time after creation, making the information inaccessible.

The risks to privacy through use of instant messaging stems from poor security associated with these devices by the user and the fact that the information goes through a server of a third party. Bring your own device policies create further privacy risks given that the line between personal and business use is blurred and the information may become intertwined.

The ability to store large amounts of personal information on mobile devices including memory cards and USB[7] flash drives has resulted in a number of privacy breaches.[8]

[6] This is known as "function creep." Function creep occurs when surveillance installed for one purpose is then used for another which often changes the use of the personal information collected in contravention of legislation resulting in a privacy breach.

5) Email

The ability to access information contained in emails has proven extremely challenging due in part to the sheer volume of emails. Email storage takes a significant amount of server space. The information in emails is unstructured making the ability to locate a record that may be responsive to an access request challenging. There are differing practices around the extent to which emails, including those backed up on servers, will be searched in response to an access request. Redaction of information severable in response to an access request electronically is not always possible, thereby extending the timelines to respond when this work must be done manually. For retention purposes, it is difficult to separate transitory emails from emails having business value.

Privacy is also negatively impacted through the use of emails. Personal information protection practices that would otherwise be applied to paper correspondence are not applied to email communications. Email communications are insecure given that the email goes through third party (including public body) servers, which is often overlooked. Breaches of privacy occur often as a result of an email being sent to the wrong party.

6) Electronic Information (EI) Systems

EI systems are being used to improve service delivery and to achieve economic efficiencies. As part of this, information is being shared within and between Public Bodies and Private Bodies, and large amounts of information about individuals are being combined.

---

[7] Universal serial bus.

[8] In September 2013, Medicentre Inc. reported the loss of a laptop containing the billing information of approximately 631,000 Albertans. The personal information on the laptop included patient name, health number, birth date, diagnostic disease codes, and health service billing codes. The laptop was password protected but not encrypted. It was not recovered. *Investigation Report H2014-IR-01 Report concerning theft of unencrypted laptop containing health information http://www.oipc.ab.ca/downloads/documentloader.ashx?id=3481.*

In March of 2011, Edmonton Public School District reported the loss of a USB stick thought to contain the personal information of 7000 individuals. It was determined that the personal information on the USB included employment applications, resumes, transcripts, completed direct deposit forms (including cheques), copies of driver's licenses, first page of passports, birth certificates, injury forms, payroll correspondence, pension correspondence, benefits forms and correspondence, education credentials, job information history, pay-benefits history, performance evaluations, and police criminal records check reports. The USB stick still was not encrypted or password protected. The USB stick was not recovered. *Report of an investigation into a missing USB Memory Stick July 27, 2011 Edmonton Public School District No. 7 Investigation Report F2012-IR-01.*

In January 2013, Human Resources and Skills Development Canada reported losing an external hard drive containing the names, social insurance numbers, birthdates and addresses of up to 583,000 students who had applied for student loans. The hard drive, which was unencrypted, was not recovered. http://blog.priv.gc.ca/index.php/category/privacy-breach/.

To improve service delivery, Public Bodies are beginning to build repositories of information using EI systems, some for identification purposes, such as citizen registries, and some for business purposes, such as management of services, including health services.

Citizen-centred service delivery is one reason that government and health care Bodies share and combine personal information using EI systems.[9] The idea behind citizen centred services is to allow the sharing and combining of information within and between these Bodies to enable them to identify a citizen's government or health care needs from birth to death. Once this data is amassed, these Bodies can use this information to inform service delivery needs for citizens to inform planning and mitigate costs to the system by ensuring the services provided focus on these needs.

Economic factors also drive the sharing and combining of information within and between government and health care Bodies where cost savings can be achieved by purchasing one information system that is utilized by a number of different programs within an entity or different entities, which often occurs in government where there are numerous Public Bodies.[10] Cost savings may also be achieved through the sharing and combining of information when resources required to deliver services are reduced and service delivery is not impacted or it is improved.

While there are benefits from developing EI systems, there are also risks to privacy, such as unintended surveillance and profiling, that could further impact other freedoms if use of the amassed information leads to authoritarian-style decision making about a specific citizen's service needs. When developing EI systems, these risks need to be identified, addressed and managed.

To effectively protect privacy, planning for privacy needs to occur when planning the information management ecosystem and for each EI system developed within this ecosystem. Privacy impact assessments (PIA),[11] which need to be completed on the information management ecosystem and for each EI system developed thereunder to ensure privacy is being effectively managed, are not always done.[12]

---

[9] An example of this is the Panorama System that is located in British Columbia and in which the public health information (personal health information of citizens who interact with public health care providers) from multiple Public Bodies in British Columbia (Regional Health Authorities, British Columbia Centre of Disease Control, Government of British Columbia Ministry of Health, First Nations' Health Authorities) and Yukon Government Department of Health and Social Services is pooled for the purposes of population health management.

[10] For example, under the ATIPP Act, each Yukon Government department is a separate public body. The Yukon Government as a whole is not a single public body under the ATIPP Act.

[11] A PIA is a tool that can be used by a Public Body or Private Body when developing and EI system in which personal information will be collected, accessed, used, retained or disclosed to evaluate the risks of noncompliance with access and privacy laws and for evaluating the overall risks to privacy versus the benefits to be achieved through use of the new EI system.

[12] An important part of completing a PIA is the evaluation and weighing of the benefits to be achieved through use of the EI systems versus the risks to privacy. Evaluating privacy impact needs to occur at the initial stages of planning to allow a change of course should the risks to privacy outweigh the benefits so that an alternate course

To ensure privacy protection is managed both during and after development of the EI system, prior to building these systems, an effective privacy management program needs to be[13] in place that includes a robust training for employees about their privacy responsibilities and auditing to ensure compliance. Many Public Bodies do not have these programs in place.

Poor privacy management has led to a number of breaches. The ease of access to information in EI systems by employees of both Public Bodies and Private Bodies has proven to entice authorized EI system users to access, use and disclose personal information improperly. Information is a wanted commodity in today's marketplace[14] and users with authorized access to EI systems have breached privacy for personal gain opportunities or other malicious purposes.[15] Adequate steps are not being taken to prevent these activities and individuals who trust these Bodies with their personal information are paying the price in the harm suffered as a result of privacy breaches.

There are risks to accessing information in EI systems, including personal information, when a new EI system is implemented. If users are not trained on how to search and retrieve records that may be responsive to a request for access to information, they may not be able to locate responsive records. If information is inadvertently deleted from an EI system or not properly retained, an individual will be unable to access the information.

7) Cloud Computing[16]

---

could be chosen that would decrease the risks to privacy and protect citizens from unnecessary and potentially harmful privacy intrusion.

[13] See "Guidance for Public Bodies on Accountable Privacy Management" for the components required by a public body to have an effective privacy management program, Yukon Information and Privacy Commissioner's website, http://www.ombudsman.yk.ca/uploads/general/Privacy_Program_Management.pdf.

[14] See comments on the new digital economy and Big Data.

[15] In two separate incidents, one in July 2013 and the other in 2014, two employees of two hospitals (Rouge Valley Centenary and Rouge Valley Ajax and Pickering) used their access to the hospital's information system (Meditech) to access information about patients who recently gave birth. This information was used by these employees to sell registered education savings plans (RESP). The investigation into these incidents found that one employee sold the patient information of 400 patients to an RESP sales agent. Fourteen thousand patients were affected by the privacy breach.

In December of 2011, a pharmacist pleaded guilty to knowingly obtaining personal health information which she used to humiliate a woman in her church as a result of romantic interests of a male member of the church congregation. The pharmacist had accessed Alberta's Netcare where she obtained prescription information about the woman and subsequently posted the information on Facebook. The investigation determined that the pharmacist also accessed medical records of eight other individuals who the woman affected by the breach identified as individuals who were sympathetic to the woman. The pharmacist was charged with 11 counts of knowingly obtaining or attempting to obtain health information in contravention of Alberta's *Health Information Act.*

[16] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models. The NIST Definition

Use of a cloud for information storage creates risks to accessing information and for privacy protection.

Most cloud service providers are situated in jurisdictions outside Canada. Cloud service providers, particularly those offering a public cloud[17], will generally offer take it or leave it contracts which severely limits the ability of Bodies to ensure the risks to privacy are properly addressed through contract: control of the personal information; restricting the collection, access, use and disclosure of the personal information by the cloud providers' employees; securing the personal information and what will occur in the event of a breach; retaining the personal information during the contract term; ensuring the integrity and accessibility of the personal information; and the return or secure destruction of the information upon termination of the contract. How the laws of the jurisdiction will impact the privacy of the personal information is also not being properly considered.

Access to information stored in the cloud may be impeded if the cloud service is unavailable[18], the information is lost, or the cloud provider goes out of business.

Commissioners Call on Governments to Protect and Promote Canadians' Access and Privacy Rights in the Era of Digital Government

In a joint resolution issued by the Commissioners in November of 2014[19], which due to its relevance is replicated below, Commissioners called on their respective Governments to protect and promote access and privacy rights contained in access and privacy laws to ensure technological developments do not erode access and privacy rights.

> *Technologies present tremendous opportunities and challenges for access and privacy rights all across Canada and all over the world.*
>
> *In fact, digital information has become the lifeblood of governments. It is the foundation of decision-making, policy development, and service delivery to citizens. Digital information is a*

---

of Cloud Computing, National Institute of Standards and Technology, Mell, P. and Grance, T., Special Publication 800-145, U.S. Department of Commerce, September 2011, p. 2.

[17] Public cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Mell, P. and Grance, T., Special Publication 800-145, U.S. Department of Commerce, September 2011, at p. 3.

[18] October 22, 2012, Flipboard, Foursquare, Netflix, Pinterest, and Instagram services were unavailable when the cloud service provider's servers went down, Amazon Cloud Service Goes Down and Takes Popular Sites With It, Perlroth, N., Bits, October 22, 2012, http://bits.blogs.nytimes.com/2012/10/22/amazon-cloud-service-goes-down-and-takes-some-popular-web-sites-with-it/?_r=0.

[19] This document can be found at: http://www.ombudsman.yk.ca/news_events/joint_resolution_from_canadas_access_to_information_and_privacy_guardians/.

pillar of open government and citizens' participation in democracy. The public expects increasingly open, responsive and efficient governments.

In parallel, official communications are increasingly done using technologies that did not exist at the time most privacy and access laws were enacted; organizations are generating unprecedented volumes of information that they must organize, store, search and secure, so as to both facilitate legitimate access and prevent unauthorized disclosures; technologies are changing the nature of government records and is challenging traditional information management practices.

Moreover, just as technology is bringing undeniable benefits to governments and society at large, digital information is now more vulnerable than paper records ever were.

With regard to privacy rights, biometrics, wearable computing devices, cloud computing and other technological developments have increased the risk of over-collection and over-retention of personal information, inappropriate sharing of personal information, data matching and data breaches.

With regard to information rights, the level of complexity in recovering information stored outside official networks, such as on personal file storage, wireless devices, in the cloud or in personal email accounts, has been compounded. At the same time, the oral culture of government and the lack of any formal duty to properly document decisions inevitably limit what records are available for access purposes.

This underlines the crucial role of responsible and modern information management law, policy and practices in protecting access and privacy rights, two essential components of our democracy.

WHEREAS

We are undergoing an unprecedented technological and cultural shift where life and communications are increasingly happening in the digital world.

The rapid development of technologies outpaces the capacity to appropriately manage both paper and digital records and to protect against loss and unauthorized access.

Current government policy frameworks and practices often prove to be not adapted to the use of new technologies, creating new risks to access and privacy rights.

The protection and exercise of information rights rests on the ability of organizations to effectively create, organize, manage, protect and preserve records.

Only responsible, strong and effective information management infrastructures and practices will allow governments to seize digital opportunities and fundamentally change how they serve the public in a more cost effective, transparent, responsive and accountable way.

It is a critical time for bold leadership from our governments to ensure the continued relevance of access to government information in a digital society, while ensuring that personal information is vigilantly protected.

THEREFORE

Canada's Privacy and Information Ombudspersons and Commissioners urge their respective governments to review and modernize their information management frameworks by doing the following:

1. *Embedding privacy and access rights into the design of public programs and systems;*
2. *Creating a legislative duty requiring government employees to document matters related to material deliberations, actions and decisions;*
3. *Adopting administrative and technological safeguards to*
    - *prevent the loss or destruction of information;*
    - *guarantee that digital records are adequately stored in designated repositories and retained for prescribed periods of time, so that they can be easily retrieved when required;*
    - *mitigate the risks of privacy breaches, which are becoming more frequent and severe;*
    - *ensure that governments collect and share only that personal information strictly necessary to achieving the objectives of given programs or activities.*
4. *Establishing clear accountability mechanisms for managing information at all steps of the digital information lifecycle (collection, creation, use, disclosure, retention and disposal) to meet privacy and access obligations, including proper monitoring and proper sanctions for non compliance;*
5. *Training all government employees involved in managing information at any stage of its lifecycle in order for them to know their roles and responsibilities, including their obligation to protect privacy and access rights, and to continue to meet those obligations in the face of new technologies;*
6. *Proactively releasing digital information on government activities on an ongoing basis in accordance with open government principles.*

The Path to Innovation

Given the changing information landscape and the technological development that has occurred since access and privacy laws came into effect, and the increased inclination for governments to use this technology to further their vision, current access and privacy laws, which were not written with the use of technology in mind, are no longer adequate. The laws, as written, can serve to stifle innovation which, in some cases, has led Public Bodies to violate the laws to achieve their objectives. Commissioners, who are aware these violations are occurring and whose responsibility it is to ensure these laws are complied with, are put in a very difficult position when trying to bring Public Bodies into compliance with the laws that most Commissioners would agree need updating to support innovation.[20]

Rather than continuing to pit Public Bodies against Commissioners in the fight over innovation versus access and privacy protection, these laws need to be updated to support innovation while also ensuring there are adequate protections in place to protect privacy and access rights.

Use of Technology by Yukon Government Public Bodies

Yukon Government Public Bodies (YG Public Bodies)[21], like their counterparts in other jurisdictions, are moving towards a citizen-centered service delivery model and are looking to use technology to support this model. They are beginning to develop system strategies and implement EI systems in support of this model. In some instances, they are seeking, through the use of technology, to combine and share personal information within and between themselves and with other Public Bodies or Private Bodies located in Yukon or elsewhere.

YG Public Bodies are looking to participate in the development of the digital economy. The Department of Highways and Public Works is moving forward with an electronic services strategy with the goal of providing government services to citizens via the Internet in support of citizen centered services. The Department of Environment recently announced that camping and fishing licenses can be purchased online.[22]

Employees of YG Public Bodies use email and mobile devices, such as cell phones, laptops and tablets, to conduct business. BYOD policies are in place that allow YG Public Body' employees to use their personal devices to conduct business.

YG Public Bodies use surveillance technology to monitor the workplace and public places.

YG Public Bodies are beginning to use cloud based services.[23]

---

[20] This is my view based on research conducted.

[21] A "YG Public Body" is a department of Yukon Government.

[22] See http://www.env.gov.yk.ca/environment-you/eServices.php.

[23] At the time of writing this letter, I am aware of one Public Body using these services.

Given that the ATIPP Act was written 20 years ago when the use of technology to manage information was not the norm, the ATIPP Act, in some cases, restricts the ability of YG Public Bodies to use technology to achieve their respective goals. Given the direction of YG Public Bodies and in recognition of the benefits and risks associated with innovation in the new electronic information era, the ATIPP Act needs to be amended to allow innovation to occur while ensuring privacy and access rights are protected.

ATIPP Act Challenges to Innovation

As YG Public Bodies move toward the objective of delivering citizen centered services, they are seeking to share and combine personal information using technology. The provisions in Part 3 of the ATIPP Act that require Yukon Public Bodies to protect privacy prevent YG Public Bodies from meeting these objectives. Specifically, sections 29 to 36 in Part 3 do not allow YG Public Bodies to combine or share personal information for these purposes.

Legislative Amendments to Facilitate Innovation

Most other jurisdictions in Canada have modified their public sector privacy laws to enable increased sharing of personal information and use of technology by Public Bodies, for enhanced service delivery. An overview of these legislative changes follows.

1. The authority to collect personal information has been expanded.

    a. Collection of personal information for certain purposes is authorized with consent of the individual the information is about and subject to specific rules about the content of the consent.[24]

    b. Collection of personal information is authorized for identity management purposes.[25]

2. The authority to disclose personal information has been expanded.

    a. Disclosure is authorized for a common or integrated program or activity[26] provided an agreement is in place to confirm that the program or activity is common or integrated.[27]

    b. Disclosure is authorized for:

[24] In British Columbia's (BC) *Freedom of Information and Protection of Privacy Act* (FIPPA) and Ontario's (ON) *Freedom of Information and Protection of Privacy Act* (FOIPPA).

[25] BC's FIPPA.

[26] In BC's FIPPA, Alberta's (AB) *Freedom of Information and Protection of Privacy Act* (FOIPPA), Manitoba's (MB) *Freedom of Information and Protection of Privacy Act* (FIPPA), New Brunswick's (NB) *Right to Information and Protection of Privacy Act* (RTIPPA), Prince Edward Island's (PEI) *Freedom of Information and Protection of Privacy Act* (FOIPP Act), and Newfoundland and Labrador's (NL) *Access to Information and Protection of Privacy Act* (ATIPPA).

[27] In BC's *Freedom of Information and Protection of Privacy Act Regulation*.

i. determining or verifying eligibility for a program, product or service,

ii. verifying accuracy of personal information, and

iii. for collecting a debt owing to the government.[28]

c. Disclosure is authorized for data linking or matching, or volume or bulk disclosures with authority from the head of the Public Body.[29]

d. Disclosure is authorized for retaining the services of an information manager provided an agreement is entered into,[30] the information manager is bound to comply with the privacy law, and the information deemed in control of the Public Body.[31]

3. The obligations of Public Bodies to protect personal information have been increased.

a. Government Public Bodies are required to evaluate whether a PIA for any proposed enactment, system, project, program or activity is required and if so must submit them internally for review. Where the PIA is in respect of a common or integrated program or activity, or data linking initiative, the PIA is required to be submitted to the Commissioner for review and comment.[32]

b. Non-government Public Bodies are required to conduct PIAs for any proposed enactments, systems, projects, programs or activities and submit them to the Commissioner for review and comment.[33]

c. Government Public Bodies are required to enter into information sharing agreements when sharing personal information.[34]

d. Ministers responsible for a privacy law are required to work with the Commissioner to develop and implement an information-sharing code of practice.[35]

e. Public bodies are required to report breaches of privacy to the Commissioner.[36]

---

[28] Saskatchewan's (SK) *The Freedom of Information and Protection of Privacy Regulations*.

[29] NB's RTIPPA.

[30] MB's FIPPA and ON's FOIPPA.

[31] MB's FIPPA.

[32] BC's FIPPA and NL's ATIPPA.

[33] BC's FIPPA.

[34] *Ibid.* 33.

[35] *Ibid.* 33.

[36] Nunavut's (NU) *Access to Information and Protection of Privacy Act* (ATIPP Act) and NL's ATIPPA.

f. Public bodies are required to protect records from unauthorized copying or modification, and to retain, transfer and dispose of records in a secure manner.[37]

g. The ability, through regulation, has been created to:

i. develop technical standards and safeguards,[38]

ii. develop data linking, data matching, and data sharing standards,[39] and

iii. establish review committees to review data linking or matching, or volume or bulk disclosures of data.[40]

4. The ability to designate an identity information service provider[41] or service provider organization[42] has been created along with clarification on what these services entail and limits placed on collection, use and disclosure of personal information for these services.[43] There is also Ministerial oversight[44]or Commissioner' audit capability[45] with respect to these services.

Details associated with these authorities and responsibilities are set out in Appendix A.

ATIPP Act Amendments to Facilitate Innovation

To enable YG Public Bodies to achieve their current service delivery goals and participate in national information sharing initiatives underway, the following is recommended:

Recommendation #1

Consideration should be given to amending Part 3 of the ATIPP Act to expand the authority of Yukon Public Bodies to collect and disclose personal information to facilitate innovation. If applicable, consideration should also be amending the ATIPP Act to authorize the creation of a service provider in a YG Public Body to be responsible for centralized citizen services.

[37] NL's ATIPPA.

[38] PEI's FOIPP Act.

[39] AB's FOIP Act and PEI's FOIPP Act.

[40] NB's RTIPPA.

[41] BC's FIPPA.

[42] ON's FOIPPA.

[43] BC's FIPPA and ON's FOIPPA.

[44] BC's FIPPA.

[45] ON's FOIPPA.

Amendments in these areas made to privacy laws in other jurisdictions should be examined to determine which amendments align with the current and future goals of YG Public Bodes and other Yukon Public Bodies.[46]

If amendments are made to the ATIPP Act to support innovation, it would be necessary to increase the obligations of Yukon Public Bodies to protect personal information.

In Part 3 of the ATIPP Act there is only one provision that addresses the protection of personal information. It states:

> *The public body must protect personal information by making reasonable security arrangements against such risks as accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal.*[47]

Having only this provision in a legislative scheme that authorizes expanded sharing of personal information between and beyond Yukon Public Bodies would not be sufficient to protect personal information. Determining the provisions that would be necessary must be considered in the specific Yukon context.

Privacy management by Yukon Public Bodies is in its infancy. Consequently, if Yukon Public Bodies are given expanded authority to collect and disclose personal information to facilitate innovation, the following is recommended to ensure the personal information will be adequately protected.

Recommendation #2

The duties of Yukon Public Bodies to protect personal information should be increased in the ATIPP Act. At minimum these duties should include:

- **a requirement that Yukon Public Bodies complete a PIA for any proposed enactment, system, use of technology, project, program or activity that involves personal information and submit them to the Office of the IPC (OIPC) for review and comment;**[48]
- **a requirement that Yukon Public Bodies notify the OIPC at an early stage of any proposed enactment, system, use of technology, project, program or activity that involves personal information, and for which a PIA will be developed, before the enactment is drafted, system acquired, or program or activity plan is finalized and consider any comments made by the OIPC with respect thereto;**[49]

[46] See Appendix A for the legislative amendments made in various jurisdictions across Canada and commentary in respect of the amendments.

[47] Section 33.

[48] This is similar to the requirements in BC's FIPPA and NL's ATIPPA.

[49] *Ibid.* 48.

- **a requirement that a PIA be completed for development of a centralized service provider and that the PIA be submitted to the OIPC for review and comment;**
- **prior to development of the centralized service provider, the OIPC is provided with the plan for centralized services before the plan is finalized and consider any comments the OIPC has about the plan;**
- **a requirement that Yukon Public Bodies enter into information sharing agreements when sharing personal information;**[50]
- **a requirement that Yukon Public Bodies submit draft information sharing agreements to the OIPC for review and comment, or a requirement that the Minister responsible for the ATIPP Act works with the OIPC to develop an information sharing code of practice;**[51]
- **a requirement that Yukon Public Bodies notify individuals about a breach of their privacy (theft, loss, or unauthorized access, disclosure or disposition of personal information) and submit a report about the breach to the OIPC for review and comment;**[52]
- **a requirement that Yukon Public Bodies make information available to the public about information sharing agreements entered into, PIAs developed, and breaches of privacy.**

Recommendation #3

The ATIPP Act should require Yukon Public Bodies to develop and maintain a privacy management program consisting of:

- **the ability to demonstrate accountability for privacy management through executive management support, designation of a privacy officer, and development of a reporting structure in respect of the privacy officer's activities;**
- **a personal information inventory and program controls: privacy policies and procedures, use of risk management tools (PIAs, security threat risk assessments, and ISAs); employee training programs and tools, service provider management, and external communications to the public including: privacy policies and procedures; notices about collection, use and disclosure of personal information, and information about rights and how to exercise them; and**
- **an oversight and review plan to identify and address deficiencies in the program.**[53]

---

[50] This is similar to the requirements in BC's FIPPA.

[51] *Ibid.* 50.

[52] This is similar to NL's ATIPPA and NU's ATIPP Act. This is also a requirement in most health information privacy laws, including the *Health Information Privacy and Management Act* (HIPMA), which have been more recently amended or enacted. This is also a requirement in the recent amendments to the Federal *Personal Information Protection and Electronic Documents Act* and AB's *Personal Information Protection Act.*

Privacy laws are more commonly incorporating these kinds of detailed privacy management program requirements to ensure personal information is properly protected. [54]

Commissioners' Oversight

An important aspect of achieving a proper balance between allowing Public Bodies to innovate through the use of technology and ensuring access and privacy rights are protected is to ensure the Commissioner has the proper authority to enable effective oversight. If amendments are made to the ATIPP Act to facilitate innovation by Yukon Public Bodies, an evaluation of whether the IPC has sufficient authority to ensure proper oversight would be required. Those jurisdictions that amended their public sector privacy laws to enable innovation by Public Bodies would have been required to conduct an evaluation of this nature. An overview of the powers granted to Commissioners in these jurisdictions follows.

General Powers Granted to Commissioners

Most Commissioners have general powers to:

- conduct own motion investigations where the Commissioner has reason to believe a Public Body is not complying with the privacy law;[55]
- conduct audits to ensure Public Bodies are complying with their obligations under the privacy law;[56]
- inform or educate the public about the privacy law; [57]
- receive comments or representations about the administration of the privacy law by a Public Body;[58]
- conduct research;[59]
- comment on the implications to privacy protection or access to information of a proposed legislative scheme or programs of Public Bodies;[60]

---

[53] See *Guidance for Public Bodies on Accountable Privacy Management* developed by the Yukon's Information and Privacy Commissioner's Office, January 2015, located at: http://www.ombudsman.yk.ca/uploads/general/Privacy_Program_Management.pdf.

[54] See, for example, NL's ATIPPA, PEI's FOIPP Act, AB's FOIP Act, NB's RTIPPA and the HIPMA.

[55] BC's, AB's, MB's, PEI's and NL's Commissioners have this power and NU's Commissioner has own motion review power.

[56] BC's, MB's, ON's, NB's and NL's Commissioners have this power.

[57] BC's, AB's, MB's, ON's, NB's, and NL's Commissioners have this power.

[58] *Ibid.* 57.

[59] BC's, AB's, MB's, ON's, and NL's Commissioners have this power.

- comment on the implications of privacy in respect of data-linking;[61] and
- authorize the collection of personal information by the Public Body from other sources.[62]

Some Commissioners also have the power to:

- deliver educational programs to inform Public Bodies about their duties;[63]
- receive comments about matters concerning access to information and confidentiality, and protection and correction of personal information;[64]
- take actions necessary to identify, promote and where possible cause adjustments to practices to improve protection of personal information;[65]
- provide assistance to individuals;[66]
- comment on the use of information technology in the collection, storage or transfer of personal information;[67]
- consult with any person with experience or expertise in any matter related to the privacy law;[68] and
- give advice and recommendations to a Public Body.[69]

Investigation and Review[70] Powers Granted to Commissioners

Most Commissioners have the power to investigate a complaint or conduct a review about a complaint made by an individual that a public body has collected, used or disclosed personal information contrary to privacy laws.[71] Commissioners with these powers commonly have the power to:

---

[60] BC's, AB's, MB's, ON's, NB's, PEI's, and NL's Commissioners have this power.

[61] BC's, AB's, MB's, NB's, PEI's, and NL's Commissioners have this power.

[62] BC's, AB's, ON's, PEI's, and NL's Commissioners have this power.

[63] NL's Commissioner has this power.

[64] *Ibid.* 63.

[65] *Ibid.* 63.

[66] *Ibid.* 63.

[67] MB's and NL's Commissioners have this power.

[68] *Ibid.* 67.

[69] AB's and PEI's Commissioners have this power.

[70] The difference between a review power and power to investigate is generally the power to review involves an inquiry, a quasi-judicial process that enables the person conducting the inquiry to make findings of fact and law.

- try and settle a complaint;[72]
- compel production of witnesses and documents;[73] and
- enter the Public Body's premises to make copies of records and have private conversations.[74]

Commissioners with review powers commonly have the power to:

- conduct inquiries where they can decide questions of fact and law;[75]
- conduct an inquiry in private;[76] and
- refuse to conduct an inquiry.[77]

The power of Commissioners to remedy non-compliance with a privacy laws differs. What is common is that most enable a binding order to be issued against a Public Body that is found to have collected, used or disclosed personal information contrary to the law.[78]

Common among Commissioners with order making powers is the authority to:

- specify any terms and conditions when making an order; [79] and
- following an audit, issue an order to enforce compliance.[80]

Common among Commissioners with only the power to recommend is they have broad powers of recommendation to remedy any non-compliance with the privacy law found following an investigation or audit, or when exercising the authority to comment.[81]

---

[71] BC's, AB's, MB's and PEI's Commissioners have the authority to investigate complaints. AB's, MB's (Ombudsman requests adjudicator to review), PEI's and NU's Commissioners have authority to review complaints.

[72] AB's, MB's and PEI's Commissioners have this power.

[73] BC's, AB's, MB's, PEI's, and NL's have this power.

[74] MB's, NB's and NL's Commissioners have this power.

[75] AB's and PEI's Commissioners have this power.

[76] PEI's Commissioner has this power.

[77] AB's and PEI's Commissioners have this power.

[78] BC's, AB's, ON's, and PEI's Commissioners have authority to issue orders. MB's Ombudsman has the authority to refer a complaint about privacy to an adjudicator if the public body does not accept the Ombudsman's recommendations following a privacy investigation. The adjudicator has order making power. Under NL's ATIPPA, if a public body declines to accept the NL Commissioner's recommendations following his investigation into a complaint about privacy, the public body is required to go to court and have the court certify they are not required to follow the Commissioner's recommendation. The court will hear the matter *de novo* and has the authority to make an order upon finding the public body contravened the ATIPPA.

[79] AB's and PEI's Commissioners have this power.

[80] BC's Commissioner has this power.

Some Commissioners have the power to publish special reports associated with their responsibilities under privacy laws.[82]

Details associated with these powers are set out in Appendix B.

ATIPP Act and IPC Oversight

The power granted to the IPC under the ATIPP Act for oversight of a Yukon Public Body's authority and responsibilities under Part 3 is limited. The IPC has authority to investigate complaints about the administration of the ATIPP Act[83] and to conduct a review of a complaint that a Yukon Public Body collected, used or disclosed personal information contrary to the ATIPP Act.[84] If following a review the IPC finds the Public Body failed to comply with any privacy requirements in Part 3, she may only recommend:

- the Public Body destroy information collected in contravention of the ATIPP Act, and
- a change the Public Body should make in its conduct so as to avoid using or disclosing the information in contravention of the ATIPP Act.

The IPC also has the power to compel appearance of witnesses and production of records[85] and during a review the IPC may try and settle a matter under review.[86] She may also conduct an inquiry and decide questions of fact and law.[87]

As for General Powers under the ATIPP Act, the IPC only has the power to:

- inform the public about the ATIPP Act;
- comment on the implications for access to information and protection of privacy of existing or proposed legislative schemes or programs of Yukon Public Bodies;

---

[81] NB's Commissioner has authority to make recommendations as part of her authority to make comments on the implications to privacy, using or disclosing personal information for a records linkage or using technology in the collection, storage, use or transfer of personal information. She may also make recommendations following an audit or on her own initiative or if requested by a public body or responsible minister about the administration of RTIPPA. There is no limit on the NB's authority to make recommendations. NU's Commissioner has the authority to make recommendations following a review of an allegation by an individual that a public body has collected, used or disclosed personal information contrary to the ATIPP Act. There is no limitation on these recommendations.

[82] MB's Ombudsman and AB's and BC's Commissioners have this power.

[83] Subsection 42 (b).

[84] Subsection 48 (3).

[85] Section 53.

[86] Section 51.

[87] Subsection 52 (1).

- authorize the collection of personal information from sources other than the individual the information is about;
- authorize persons or classes of persons to enter into arrangements or agreements under the *Health Act*; and
- report to a Minister information and the IPC's comments and recommendations about any instance of improper administration of the management or safekeeping of a record in the custody or control of a Yukon Public Body.[88]

The powers granted to the IPC under the ATIPP Act do not include the powers commonly granted to Commissioners previously mentioned, such as the power to:

- conduct own motion investigations where the Commissioner has reason to believe a Yukon Public Body is not complying with the ATIPP Act;
- conduct audits to ensure Yukon Public Bodies are complying with their obligations under the ATIPP Act;
- comment on the implications of privacy in respect of data-linking;
- enter a Yukon Public Body's premises to make copies of records and have private conversations; and
- issue an order or make any recommendations necessary to remedy non-compliance or in respect of any power granted.

The ATIPP Act does not provide any remedy for non-compliance with Part 3 where a Yukon Public Body decides not to accept a recommendation made by the IPC.

ATIPP Act Amendments to IPC Oversight

In determining what powers to grant the IPC to ensure there is effective oversight of the authorities and responsibilities granted to Yukon Public Bodies to facilitate innovation through the use of technology under Part 3, it is necessary to consider the specific Yukon context.

There are no powers in the ATIPP Act that would authorize the IPC to examine the risks to privacy as a result of systemic issues in Yukon Public Bodies which are commonly caused by poor privacy management practices. Investigating and reviewing complaints about privacy does not address systemic issues.

Yukon Public Bodies have been very slow in developing privacy management programs. Consequently, the risks to privacy are significant as a result of poor, or non-existent, privacy management practices. Some Yukon Public Bodies are beginning to develop these programs and some are not. Some Yukon

[88] Section 42.

Public Bodies develop PIAs on programs and EI systems and submit these PIAs to the OIPC for review and comment while others do not.

Completing a PIA enables a Yukon Public Body to recognize the risks to privacy and develop strategies to mitigate those risks. For the most part, Yukon Public Bodies work with the OIPC to identify and address privacy risks. There have been instances, however, where the risks are not mitigated to the satisfaction of the IPC, or at all, prior to use of the system or start of the program.

The cost of modifying or altering a system or program, or delaying the use or start, to ensure privacy protection can be significant. Where a recommendation is made by the IPC that results in significant costs, a Yukon Public Body may be less inclined to accept that recommendation. Many PIAs are not submitted to the OIPC until the system is purchased and implementation is imminent.

The importance of ensuring a Commissioner has powers to address systemic issues was discussed in the Report issued by the Committee that recently reviewed Newfoundland and Labrador's ATIPPA (NL's ATIPPA Review Committee). On this point, citing a majority decision of the Supreme Court of Canada in *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General*), NL's ATIPPA Review Committee wrote:

> ***The Information Commissioner and the Privacy Commissioner benefit not only individuals who request access or object to disclosure, but also the Canadian public at large, by holding the government accountable for its information practices.*** *As this Court has emphasized in the past, the Commissioners play a crucial role in the investigation, mediation, and resolution of complaints alleging the improper use or disclosure of information under government control: Lavigne, at paras. 37-39. Also, as former Justice La Forest notes in a recent report entitled The Offices of the Information and Privacy Commissioners: The Merger and Related Issues, Report of the Special Advisor to the Minister of Justice (November 15, 2005), at pp. 17-18,* ***the role and responsibilities of the Commissioners extend even further to include auditing government information practices, promoting the values of access and privacy nationally and internationally, sponsoring research, and reviewing proposed legislation.*** [89] [Emphasis in original.]

To ensure there is effective oversight by the IPC of Yukon Public Bodies expanded authority and responsibilities to facilitate innovation under the ATIPP Act, the following are recommended.

Recommendation #4

The IPC should be given the following additional general powers under Part 4 of the ATIPP Act to:

- **conduct own motion investigations where the IPC has reason to believe a Yukon Public Body is not complying with the ATIPP Act;**

[89] Report of the 2014 Statutory Review, Access to Information and Protection of Privacy Act, Newfoundland and Labrador, Volume II: Full Report, Wells, C., Letto, D, and Stoddart, J., March 2015, p. 203.

- **conduct audits to ensure Yukon Public Bodies are complying with their obligations under the ATIPP Act;**
- **comment on the implications to privacy in respect of data-linking; and**
- **comment on use of information technology in the collection, storage or transfer of personal information.**

Recommendation #5

The IPC should be given the power under Part 4 of the ATIPP Act to share personal information as necessary with other Commissioners offices for the purposes of conducting joint investigations or audits.

Recommendation #6

Consideration should be given to granting the IPC the power under Part 4 of the ATIPP Act to provide education to inform Yukon Public Bodies about their duties[90] and give advice to a public bod. These powers would be beneficial for promoting improved privacy management practices in Yukon Public Bodies.[91]

The ombuds model of recommendation power granted to the IPC under the ATIPP Act has, for the most part, worked effectively throughout the years as it relates to the IPC's powers of investigation and review. Yukon Public Bodies generally work cooperatively with the OIPC to resolve complaints and recommendations are accepted. Given this, the ombuds model should be maintained for investigation and review as it relates to the powers of the IPC with the following recommended variations.

Recommendation #7

The IPC should be given the power under Part 4 of the ATIPP Act to:

- **make any recommendations necessary to remedy any non-compliance with the ATIPP Act in respect of any power granted;**
- **publish investigation and review reports including recommendations made; and**
- **publish special reports in respect of any authority granted under the ATIPP Act.**

Recommendation #8

The powers granted to the IPC for reviews under section 53 of the ATIPP Act should be expanded so they apply to all the IPC's powers including the power to comment and audit.[92]

[90] NL's Commissioner has this power.

[91] AB's and PEI's Commissioners have this power.

[92] This power is granted to NL's Commissioner under NL's ATIPPA in subsection 95 (3).

Recommendation #9

The ATIPP Act should enable a binding order to be issued following an investigation, review or audit by the IPC where the IPC finds a Yukon Public Body to have contravened or is contravening the ATIPP Act, the Public Body refuses to comply with the IPC's recommendation to remedy the non-compliance, and the IPC is of the view that there is a significant risk to privacy as a result of the non-compliance.

To enable a binding order to be issued:

- the ATIPP Act could require Yukon Public Bodies to comply with recommendations made by the IPC to remedy non-compliance with the ATIPP Act following an investigation, review or audit unless the Yukon Supreme Court certifies it is not required to follow the recommendations,[93] or
- the ATIPP Act could authorize the IPC to refer a finding of non-compliance following an investigation, review or audit to an arbitrator for review, and following the review the arbitrator would have authority to issue a binding order against a Yukon Public Body to remedy any non-compliance found.[94]

Use of Technology Impact on Information Management

Increased use of technology by Public Bodies and poor information management practices has made the ability to access information in the custody or control of Public Bodies increasingly difficult due to the lack of information available or difficulty in locating and retrieving the information.

Under Part 2 of the ATIPP Act, the public has a right to access information in the custody or control of Yukon Public Bodies. Individuals also have the right under this Part to access personal information about themselves. There are no requirements in the ATIPP Act or in any other Yukon legislation that would require Yukon Public Bodies to manage information such that the public and individuals are able to effectively exercise these rights. If the ATIPP Act is amended to allow increased use of technology for innovation, consideration should be given to increasing the responsibilities of Yukon Public Bodies to more effectively manage information to facilitate access rights.

NL's ATIPPA Review Committee stated the following about the need to ensure Public Bodies effectively manage information to ensure the right to access information under NL's ATIPPA can be exercised.

> *The connection between quality record keeping and the successful completion of access requests is well documented.*
>
> *Information is being created today at an unprecedented rate…Much of the information being created may be stored in locations outside of the public authority's network…implementing a system by which information is managed and preserved will facilitate ease of access and retrieval, so that this information can ultimately be disseminated for the public good.*

[93] This is similar to the requirement in NL's ATIPPA.

[94] This is similar to the power granted to the Ombudsman in MB's FIPPA.

The Model Access to Information Law developed by the Organization of American States speaks to the importance of strong information management in its guide for implementing the Model Law:

> *The other part of this equation, the duty to document is a term gaining status in government and information management circles. It has become a rallying cry for Information and Privacy Commissioners and, it seems, for good reason: how can Information and Privacy Commissioners properly oversee access to information and privacy law in the absence of good records or, in some cases, no records at all?*[95]

NL's Public Body Information Management Scheme

NL's ATIPPA Review Committee noted the following about the information management scheme in place for NL's Public Bodies.

The ATIPPA assumes that records have already been created and does not address how records should be managed, apart from the duty to protect personal information.

The Management of Information Act (MOI) Section 6 provides the authority.

> *6.(1) A permanent head of a public body shall develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records."*

The MOI provides for a process to dispose of government records and a penalty of up to $50,000 for anyone unlawfully damaging, mutilating, or destroying a government record. There is also provision for the retention of electronic records.

The information management system is overseen by the Office of the Chief Information Officer (OCIO), under the legal framework of the MOI. Accordingly, the OCIO policy framework applies to all records "regardless of physical format or characteristics."

A Frequently Asked Questions section on the OCIO website explains that instant messages (Pin-to-Pin, Blackberry Messenger, SMS Text Messaging) are to be preserved in this context:

> *If you feel that the content…should be retained as a government record, it is your responsibility to transfer it to an appropriate medium.*

There is similar guidance from the OCIO with respect to email: Thus, email is a government record when it is created or received in connection with the transaction of Government business (e.g. when it records official decisions; communicates decisions about policies, programs and program delivery; contains background information used to develop other Government documents; etc.).

[95] *Ibid.* 89, p. 309.

Government records may not be destroyed without the authorization of the Government Records Committee, as outlined in the MOI.

The OCIO's policy framework outlines the responsibility "employees and contractors" have in maintaining an effective information management system. It states employees are responsible for managing and protecting records that they have created or collected; it outlines the necessity of employing physical and technical means to protect records from unauthorized access; and it states that employees who willfully breach confidentiality of personal information are open to consequences "up to and including dismissal."[96]

The key points highlighted by NL's ATIPPA Review Committee under the heading "What we heard" with respect to the need for improved information management practices by Public Bodies are as follows:

Strong information management policies and practices are the foundation for access to information. Without those policies and practices, there is no certainty that the information being requested exists, or that it is usable even if it does exist.

Canada's Information Commissioner, Suzanne Legault, recommended a legal duty to document decisions, "including information and processes that form the rationale for that decision". Commissioner Legault noted that without such a legal requirement, there is no way to ensure all information related to the decision making process is recorded. She was also concerned "the risk is compounded by the advent of new technologies used in government institutions such as instant messaging".

Without the proper creation and management of records, any statutory right of access to records will prove unenforceable in practice. Good records management goes beyond the ability to locate records efficiently. It is also concerned with how and which records should be created, how long they should be retained, and with their ultimate disposition—usually destruction or transfer to archives.[97]

New technology has made it easy to create and store records, and, unfortunately, easy to dispose of them. An example of this was reported on by the Ontario Information and Privacy Commissioner in June 2013. She found there was "indiscriminate deletion" of emails to and from the former Chief of Staff in the Ministry of Energy, related to the cancellation and relocation of gas plants in Ontario. Among other recommendations, Ann Cavoukian recommended Ontario legislate "duty to document communications and business-related activities within [the province's access and protection of privacy laws], including a duty to accurately document key decisions."

The federal government issued a directive on record keeping in June 2009, three years after the Department of Justice reported that "information management in the government of Canada

[96] *Ibid.* 89, p. 310.

[97] *Ibid*. 89, citing BC's Commissioner's "*Special Report: A Failure to Archive,* 22 July 2014, p. 6."

has declined alarmingly over the past three decades." The 2009 directive set out the goals for improved record keeping, a system of monitoring, and a promise to review performance within five years.

If there were a legislated duty to document, the provincial government could also pursue a range of sanctions to ensure that officials meet their legal duty to create and maintain records, and to discourage wilful attempts to fail to create records. Provincial sanctions could range from administrative disciplinary action to being charged with an offence.

The conclusion reached by NL's ATIPPA Review Committee in respect of the need for Public Bodies to improve information management practices in support of the NL's ATIPPA was as follows.

As of January 2015, the ATIPPA has been in place for a decade. Most of the public focus has been on the provisions of the Act that provides or restricts access, and on the practices around its administration. However, it must be realized that the ultimate success of the ATIPP system rests on its ability to manage and protect information.

Senior officials must ensure that appropriate resources are allocated to do the job completely, and that all public bodies understand the essential role that information management plays in ATIPP.

Following this conclusion, NL's ATIPPA Review Committee made the following recommendations.

- *The Government take the necessary steps to impose a duty to document, and that the proper legislation to express that duty would be the MOI, not the ATIPPA.*
- *Implementation and operation of this new section of the MOI be subject to such monitoring or audit and report to the House of Assembly by the OIPC as the Commissioner considers appropriate.*
- *Adequate resources be provided to public bodies served by the OCIO, so that there is consistency in the performance of information management systems.*

Yukon Government's Information Management Scheme

The ATIPP Act, like NL's ATIPPA assumes that records have already been created and does not address how records should be managed by Yukon Public Bodies, apart from the duty to protect personal information.

The obligations regarding information management for Yukon Government "departments and agencies" are set out in the *Archives Act* and the *Records Management Regulations* (RM Regulations). The responsibility of Yukon Government departments and agencies to manage information is set out in sections 3 and 4 of the RM Regulations.

Section 3 and 4 establishes the interdepartmental Records Management Committee.[98] The terms of reference for the Records Manager Committee are to:

> *(a) promote and develop records management within Yukon Government;*
>
> *(b) initiate and approve records management standards and guides;*
>
> *(c) review and assess Records Schedules prior to implementation;*
>
> *(d) submit, from time to time, but not less than once a year, a report to Management Board*.

The process to dispose of Yukon Government records is contained in section 6 of the *Archives Act*, which states:

> *6. Subject to the regulations no public records shall be destroyed or permanently removed without the knowledge and concurrence of the archivist.*

Section 5 and 6 of the RM Regulations state that:

> *5. (1) A Records Schedule shall:*
>
> *(a) be used to authorize (ii) the destruction or other disposal of public records;*
>
> *(b) be developed jointly by the Departmental Records Officer, the Records Manager and the Archivist, or their designates;*
>
> *(c) describe adequately the series of public records that are scheduled, including their retention periods and eventual disposition;*
>
> 6. (1) *Records Schedules will be reviewed by the Records Management Committee and (2) signed by the Archivist on behalf of the Committee.*

Sections 7 and 8 of the RM Regulations identify who is responsible for reviewing the records schedules and section 9 provides that the schedule must be in the Form 1 included in the RM Regulations.

GAM Directive 2.14 provides the following in relation to how information is to be managed by Yukon Government departments.[99]

---

[98] Membership of the Records Management Committee is: the archivist who is the Chairman, the Records Manager who is the Vice-Chairman and Secretary, Secretary to Cabinet, one representative from each of Systems and Computing Services from the departments of Finance and Justice, and other public servants invited by the committee.

[99] GAM Policy 1.1 indicates GAM policies apply to the Executive Council Office, Community Services, Economic Development, Education, Environment, Energy Mines & Resources, Finance, Health and Social Services, Highways and Public Works, Justice, Tourism and Culture, Workers' Compensation Health and Safety Board, Yukon Development Corporation, Yukon Housing Corporation, Yukon Liquor Corporation, and the Women's Directorate. These are all Yukon Public Bodies.

- "Record" "is as defined in the ATIPP Act and the *Archives Act."*

- In section 2.1, the Information Resource Management Committee (IRMC) (a subcommittee of the Deputy Minister's Review Committee) is "charged with promoting and coordinating a corporate perspective on information management."

- In section 2.2 the departments are responsible, *inter alia*, for "managing their records to meet the public policy requirements set out in the FAA, The *Archives Act,* the *ATIPP Act*, and other acts and regulations that may affect their specific programs and records."

- In section 2.3 the Department of Highways and Public Works, Information and Communications Technology Division is responsible to support the activities of the IRMC and helping departments achieve their goals by, *inter alia*, "providing insights and guidance on the application of information management principles to various technology tools that are used to manage information."

- In section 2.4, Yukon Archives is responsible to approve final disposition of records and provide advice, training and assistance to departments to help them meet their goals.

In section 3.1.2 of GAM Policy 2.24 it states that:

> *Each Deputy Minister shall implement explicit protocols, appropriate to the departments, to ensure that the department can demonstrate accountability for complying with the access, protection of privacy and other provisions of ATIPP.*

The Personal Devices policy, which authorizes Yukon Government employees to use their own personal device to conduct Yukon Government business, states the following.

> *Employees who use personal devices for work purposes must be aware that:*
>
> *Corporate information (which includes information belonging to the Government of Yukon and information about clients or other 3rd parties) which is transferred to or stored on a personal device remains under the control and custody of Government of Yukon and is subject to the ATIPP Act, the Archives Act and other legislation.*

As previously mentioned, Yukon Government records may not be destroyed or permanently removed without the knowledge and concurrence of the archivist.[100]

Yukon Government employees are required in accordance with GAM Policy 2.15, section 3.4.1, to "ensure that the necessary security precautions are taken to protect the status of records classified as confidential or exempt."[101] Sections 3.4.2 to 3.4.5 of this policy impose additional requirements on these employees to ensure information they handle is adequately protected.

[100] Section 6 of the *Archives Act.*

[101] See sections 2.1.2.1 and 2.1.2.2 of GAM Policy 2.15 for the definitions of confidential or exempt records.

The Computer Use Guidelines establish guidelines for use of Yukon Government computers and electronic networks. The responsibilities of employees of Yukon Government in respect of these computers and electronic networks include the protection of Government information and a requirement to uphold all legal and policy obligations. Section 7 of the Guidelines indicates that a failure to comply with the guidelines may result in disciplinary action up to and including dismissal.

Comparison of Information Management Schemes

The information management scheme in place for Yukon Government departments, on comparison, is not as broad as that in place for NL's Public Bodies. Of particular note is the following.

- There is nothing in Yukon Government's information management scheme that includes, as part of the scheme, a requirement to create government records as is the case in NL's MOI.[102]

- There are no financial penalties for damaging, mutilating or destroying a government record. The consequences for Yukon Government employees as it relates to information management is set out in the Computer Use Guidelines where it indicates that employees may be terminated for failure to comply with the Guidelines. These Guidelines apply only to the use of computers and electronic networks.

- There is no policy, procedure or guidance available to Yukon Public Bodies specifically addressing the use of instant messaging features on cellular telephones or other mobile devices used by Yukon Public Body employees. Nor is there anything that would require an employee of Yukon Government to ensure information stored on a mobile device is transferred for management in accordance with the *Archives Act,* RM Regulations, and applicable GAM directives and policies.

- The Personal Devices policy is narrowly focused on employees who choose to use their own cellular phone or other mobile device to conduct government business. The policy is silent on the duty of the employee to ensure government information stored on the personal device is transferred to Government information management systems.

- There is currently no policy, procedure or guidance specific to the management of emails.[103]

In a document[104] authored by the records manager for Yukon Government dated April 2011, it states the following about management of electronic records by Yukon Government.

---

[102] Subsection *6.(1) of the MOI states "A permanent head of a public body shall develop, implement and maintain a record management system for the **creation**, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records." [My emphasis.]*

[103] Yukon Government is participating in the development of an email management strategy undertaken by the Information Management Subcommittee of the Public Sector CIO Council.

[104] Access to Information and Protection of Privacy (ATIPP) Act GUIDE FOR MANAGERS, Records Manager, Department of Highways and Public Works, April 2011, p. 20.

The electronic information systems presently in use by government generally are not managing records according to generally accepted records management practice. As a result, departments continue to maintain parallel paper systems to meet legal requirements. The electronic records are nevertheless subject to ATIPP, and the flaws in treating electronic records differently from paper records are increasingly being understood.

This situation has developed in part because the formal records management frameworks currently in existence were not developed to support electronic records management. Many common electronic tools are not capable of complying with such a framework in any case.

The Information and Communications Technology Division (ICT) some years ago conducted a "readiness assessment" to determine where departments stood in terms of established record management standards and practices.

The name currently used to articulate these is GARP (Generally Accepted Records Principles), which also positions departments to prepare for managing electronic records. The readiness assessment revealed that the biggest obstacle to having and a prerequisite for using, compliant electronic systems is the lack of formal records management frameworks and not the lack of appropriate electronic tools, which had normally been seen to be the case.

In response to this, ICT has established a special project unit of about 12 people to help departments improve their records management practices through additional training and the adoption of GARP. This team has a plan to train departments in GARP over a period of the next five years, but it will be up to departments to find resources and carry out change management within their programs. ICT is following up with a strategy for managing electronic records that will be available to those departments that have adopted and are actively using GARP.

ATIPP Act Amendments to Improve Information Management

As was noted by NL's ATIPPA Review Committee, it is essential for Public Bodies to have strong information management practices comprised of policies and procedures that ensure decisions made by Government employees are documented and accessible to the public. Without strong information management practices, the public will be denied their right to access Government information or their own personal information under public sector access to information laws.

Yukon's ATIPP Act has been in effect for 20 years, which is a sufficient amount of time for Yukon Public Bodies to develop strong information management practices that support citizens' rights to access information under the ATIPP Act. While some work has been done toward this objective, as is demonstrated above, there is much more work to be done in support of access rights under the ATIPP Act, particularly in light of the increased use of technology by Yukon Public Bodies to manage information.

To ensure information is properly managed by Yukon Public Bodies so that the public and individuals are able to exercise their right to access information under the ATIPP Act, the following is recommended.

Recommendation #10

The ATIPP Act should require Yukon Public Bodies to apply information management practices that include development of policies and procedures in support of the right to access information. At minimum these requirements should include:

- **a requirement that Yukon Public Bodies develop policies and procedures to ensure that:**
  - **deliberations and actions undertaken and any decisions made by an employee that relates to his or her employment responsibilities are documented;**
  - **recorded information that is stored outside the Public Body's information management system, including on any mobile electronic devices, that is not transitory is transferred to the Public Body's information management system within a specified period after creation of the record;**
  - **there are clear consequences for employees who fail to comply with the policies and procedures; and**
  - **before a decision is made to acquire technology on which information will be stored, the Public Body consider the impact on access to information rights and evaluate whether the benefits of using the technology outweigh removal of access to information rights, and that this decision and the reason for the decision are documented and retained for a specified period;**[105]
- **a requirement that Yukon Public Bodies consult with the IPC during the development of information management policy and procedure**.

[105] This issue has come up a number of times in the OIPC where individuals request access to information recorded as a result of video surveillance and the request for access to the video record denied by the Yukon Public Body with custody or control of the record for the reason that they are unable to redact personal information from the video record in order to provide access. Technology exists that would enable redaction of personal information from video records. Had the requirement to evaluate the impact on access rights existed when the video surveillance equipment been acquired, the public body would have chosen the technology that allows redaction or been required to justify purchasing equipment that removes access rights.

RETHINKING THE ROLE OF THE RECORDS MANAGER

Yukon is the only jurisdiction in Canada with that has a records manager as part of its access to information regime. In Yukon, to access information in the custody or control of a Yukon Public Body under Part 2 of the ATIPP Act, a person must make a request to the records manager. The records manager and each Yukon Public Body has responsibilities associated with a request for access to records that are set out in sections 6 to 13 of the ATIPP Act. A description of these responsibilities and how they are carried out follows.

The records manager is structured such that he receives requests for access to information under the ATIPP Act from the public or individuals (Applicants) and forwards the requests on to the Public Body that has custody or control of the records requested.[106]

The records manager then writes to the Applicant and provides the Applicant with the date by which he must respond to the request for access.[107] He also provides a date to the Public Body by which it must provide him with its response to the access request.[108]

If the Public Body is unable to provide him with a response by the date indicated, the records manager is informed of the reason. The records manager may extend his time to respond if any of the circumstances in section 12 (1) apply.

> ***12****(1) The records manager may extend by up to 30 days the time for responding to a request if*
>
> *(a) the applicant does not give enough detail to enable the public body to identify a requested record;*
>
> *(b) a large number of records is requested or must be searched and meeting the time limit would unreasonably interfere with the operations of the public body;*
>
> *(c) the public body needs more time to consult with a third party or another public body before deciding whether or not to give the applicant access to the record;*
>
> *(d) a third party asks for a review under section 48; or*
>
> *(e) multiple concurrent requests have been made by the same applicant or multiple concurrent requests have been made by two or more applicants who work for the same organization or who work in association with each other, and meeting the time limit would unreasonably interfere with the operations of one or more public bodies.*

The records manager may extend his time to respond another 30 days if deemed reasonable in the circumstances. The same process described above is used.[109]

---

[106] Sections 6 and 9.

[107] Not a requirement in the ATIPP Act but is done procedurally.

[108] Section 9.

If the records manager extends his time to respond, he is required to tell the Applicant the new date he will respond and the reason for the time extension.[110]

Upon receiving the request for access to records, the Public Body is responsible for deciding "what the response is to be," i.e., whether or not access is provided, and if not provided, the section the Public Body is relying on to refuse access. The Public Body then provides its response to the records manager.

If the Public Body determines there is third party information contained in the request, it is the records manager's responsibility to notify the third party about the request and provide a time frame in which the third party may provide written representations to the records manager as to why the information should not be disclosed. The records manager must inform the Applicant about the third party notification and also inform the Applicant that the public body will make a decision about whether to release the records to the Applicant within 30 days.[111] The records manager must then provide a written notice to the Applicant and the third party notifying them of the Public Body's decision. If the Public Body decides to release the records, the records manager must notify the third party that the records will be released to the applicant unless, within a specified time period, the third party requests the IPC to review the Public Body's decision.

The responsibility to provide a response to the Applicant's request for access to information rests with the records manager.[112] The response he provides to an applicant must contain certain information.

> *13(1) In a response under section 11, the records manager must tell the applicant*
>
> *(a) whether or not the applicant is entitled to access to the record or to part of the record;*
>
> *(b) if the applicant is entitled to access, where, when and how access will be given; and*
>
> *(c) if access to the record or to part of the record is refused,*
>
> > *(i) the reasons for the refusal and the provision of this Act on which the refusal is based,*
> >
> > *(ii) the title, business address and business telephone number of an officer or employee of the public body who can answer the applicant's questions about the refusal, and*
> >
> > *(iii) that the applicant may ask for a review under section 48.*

In providing a response to an Applicant, the records manager has the ultimate responsibility to "make every reasonable effort to assist Applicants and to respond to each Applicant openly, accurately and

---

[109] Subsection 12 (1.1)

[110] Subsection 12 (2).

[111] Sections 26 and 27.

[112] Section 11.

completely" while the Public Body's responsibility is only to assist the records manager meet this obligation.[113]

When *Bill 77, Access to Information and Protection of Privacy Act* was being debated in the Legislative Assembly, the following comments were made in respect of the purpose of Bill 77 and the role of the archivist.[114]

> *What this legislation is supposed to do is move us away from bureaucratic, secretive culture to one of openness and accessibility for citizens*.[115]
>
> *The proposed bill gives the archivist a role as a facilitator of access requests...This has been done for the convenience of the public. Members of the public do not have to figure out which department to go to for the information they want; they can go through one person.*
>
> *They can go to one place - Yukon Archives - and the staff there will ensure that their request gets to the appropriate department or departments.*[116]
>
> *…the archivist…is there to help facilitate requests… I see the archivist strictly as a facilitator to handle the requests so that people are not running all over government trying to get access to information. I think this will make it simpler for the public and I think it is a very workable solution.*[117]

In 2002 the ATIPP Act was amended by *Bill 60, An Act to Amend the Access to Information and Protection of Privacy Act*. As part of these amendments, the archivist's responsibilities were repealed and replaced with those of the records manager. The comments in respect of this amendment follow.

> *…this act — assigns many procedural responsibilities to the archivist. This amendment simply reassigns those procedural responsibilities to the records manager. The reason for this change is that the vast majority of information involved in access to information requests resides in the active records of the government, as opposed to those that are preserved in the archives.*[118]
>
> *Under renewal, primary responsibility for access to information and protection of privacy matters was transferred from the libraries and archives branch of the Department of Education*

---

[113] Sections 7 and 10.

[114] Yukon Legislative Assembly, 28th Legislative Assembly, Second Session, Spring Sitting, 1995, Hansard.

[115] Mr. Penikett, former Member of the Legislative Assembly (MLA), Yukon Legislative Assembly, 28th Legislature, Second Session, Spring Sitting, Hansard, April 24, 1995.

[116] Honourable Mr. Ostashek, former MLA, Yukon Legislative Assembly, 28th Legislature, Second Session, Spring Sitting, Hansard, April 25, 1995.

[117] *Ibid*. 116, May 1, 1995.

[118] Honourable Ms. Duncan, former MLA, Yukon Legislative Assembly, Legislative Assembly, 30th Legislature, Second Session, Spring Sitting, Hansard, April 25, 2002.

to the records management branch of the Department of Infrastructure. This change was made to improve service…[119]

This particular change, again to the Access to Information and Protection of Privacy Act, was made so that the person who actually deals with the ATIPP requests…from the public is someone who is familiar with the government's records and has good day-to-day contacts with all the departmental staff who manage those records. This is important in terms of delivery of service. It will simplify the internal communications involved in dealing with requests and improve government's ability to respond quickly to simple requests.[120]

Bill No. 60 is strictly a procedural matter dealing with how information requests are processed. So this is the nuts and bolts of how better service can be provided in making sure that the legislation matches up with the service improvement. It has no impact on the rights and responsibilities that are enshrined in the act. Those remain unchanged. It is a straightforward change to provide better service delivery.[121]

It will simplify the internal communications involved in dealing with the requests and improve government's ability to respond quickly to simple requests.[122]

It appears, based on these comments, that the role of archivist in the ATIPP Act was developed initially for the convenience of the public. A single place the public could go to make a request for access to information for any Yukon Public Body. The purpose of the archivist, as indicated in the comments, was to facilitate requests for access to information. The reason provided for transferring the responsibilities from the archivist to the records manager who is within Yukon Government was to improve service delivery. It was expressed in the comments that the change had no impact on the rights and responsibilities enshrined in the ATIPP Act.

While it is true that the public only has to go to the records manager to request access to a record in the custody or control of Yukon Public Bodies and that this may be convenient, use of the centralized records manager model, with the current responsibilities under the ATIPP Act operating within its current structure, may be negatively impacting on access to information rights under the ATIPP Act.

The responsibilities of the records manager under the ATIPP Act for responding to access requests creates issues of accountability by Yukon Public Bodies in managing and responding to access requests and causes delays in processing an access request. Additionally, due to the current structure of the records manager within Yukon Government, the records manager is viewed merely as an administrator which has resulted in the inability of the records manager to effectively perform the responsibilities set out in the ATIPP Act.

---

[119] *Ibid.* 118.

[120] *Ibid.* 118.

[121] *Ibid.* 118.

[122] *Ibid.* 118.

Records Manager and Public Body Accountability

Placing the records manager between the Applicant who is requesting access to records and the Yukon Public Body who has custody or control of the records creates an accountability gap. All contact with the Applicant is through the records manager and the obligation to respond in time, extend the time for response, and provide a complete response rests with the records manager, not the Public Body. As such the Public Body has no direct accountability for its response to an Applicant. Several problems arise as a result of this accountability gap.

Without direct communication with the Applicant, the Public Body may interpret a request for access to records received from an Applicant via the records manager narrowly or improperly with the result being that the Applicant does not receive the records requested.[123] It is the records manager's, not the Public Body's obligation, to respond to the Applicant in time and to do so openly, accurately and completely.

If a Public Body fails to provide the records manager with the information in the requisite time, it is the records manager, not the Public Body, who will violate the ATIPP Act for failing to respond in time. When this occurs, the Applicant is denied timely access to the information requested. The records manager has no control over the Public Body and cannot compel or require the Public Body to provide the information needed to provide the response in time.[124]

A similar problem arises for extensions. The records manager may find that the Public Body has not given a sufficient reason to extend *his time* to respond if a Public Body does not meet with one of the circumstances required for extension. When this occurs, the records manager is faced with the choice of extending without authority or not responding in time. Either choice made by the records manager will mean violating the ATIPP Act and denying the Applicant the right to receive timely access to the information requested.

The response provided by the Public Body may not be sufficient for the records manager to meet the obligation under the ATIPP Act to provide a response containing all the information required under section 13, which is intended to allow an Applicant to evaluate whether the Public Body has applied the ATIPP Act correctly. A failure to provide this information to the Applicant is a violation of the records manager's obligations, not the Public Body's.[125]

Where any of the foregoing situations arise, the impact is borne by the Applicant who will be denied timely access to records, access to records or information contained in records, and the ability to evaluate from a response received whether the Public Body properly applied the ATIPP Act.

---

[123] The OIPC has mediated requests for review where this was found to have occurred.

[124] See Inquiry Report File ATP13-037AR for a discussion by the IPC about the records manager's responsibilities under the ATIPP Act.

[125] See Investigation Report Files ATP14-017AI and ATP14-019AI where the IPC found this to have occurred in two separate requests for access to information. The OIPC is currently monitoring response letters received to evaluate compliance with section 13 of the ATIPP Act by the records manager.

Records Manger and Time Delays

The role of the records manager in relation to communication with the Applicant, Yukon Public Bodies and, third parties (where applicable), has the potential to create significant delays in providing a response to Applicants. The amount of back and forth between the records manager, the Public Body, the Applicant and third parties can only serve to lengthen the time for Applicants to receive the information requested. Any difficulty experienced by the records manager reaching any of the parties will only add to the time.[126] Time delays in accessing information in the custody or control of a Public Body is a significant issue and processes that create additional delays should be avoided.

Records Manager, a Facilitator

The records manager has specific accountabilities under the ATIPP Act and is not, therefore, just a facilitator of access to information requests. The records manager has specific obligations in the ATIPP Act that must be performed to ensure citizens have timely and complete access to information in the custody or control of Yukon Public Bodies.

When the role of the records manager was created, the Manager of Information Management became the first records manager. The position of records manager continues to be at a manager level. The level of the position held by the records manager has created some challenges for the records manager in meeting the ATIPP Act obligations. The result has been the adoption of administrative practices that are not compliant with the ATIPP Act. Practices, such as extending the time to respond without authority and providing incomplete responses have been adopted as a measure to more effectively work with Yukon Public Bodies in processing access to information requests.[127]

The information provided here is not intended to be critical to the incumbents in the role of records manager over the years. Rather, it is intended to highlight that the role of records manager and its current position within Yukon Government has made the obligations of the records manager in the ATIPP Act very difficult to fulfil.

ATIPP Act Amendments Re: the Records Manager

To address the adverse impacts the role is having on access to information rights, the following is recommended.

Recommendation #11

The responsibilities of the records manager in the ATIPP Act should be eliminated or significantly reduced.

The following options are provided for consideration.

1. Eliminate the records manager from the ATIPP Act.

[126] This problem has arisen when ATIPP Coordinators are away and there is no coverage by another employee.

[127] See Investigation Report Files ATP14-017AI and ATP14-019AI and Inquiry Report File ATP13-037AR.

As previously mentioned, no other jurisdiction in Canada has a records manager role in any access to information laws: public, private or health sectors. Yukon has a small number of Yukon Public Bodies which are located primarily in Whitehorse, which is a small city. Having to make a request for access to information to Yukon Public Bodies would be much less onerous in Yukon than in a province with much larger cities and Public Bodies that are widely spread out. Eliminating the records manager altogether from the ATIPP Act would eliminate the negative impacts on access to information rights created by having a records manager and place accountability for responding to access requests where it should be, directly with Yukon Public Bodies.

The landscape for access to information in Yukon will change once the HIPMA is in effect. A person wanting to access to their own personal health information under the HIPMA will need to go to each custodian[128] that has custody or control of their information to obtain access. This new landscape supports eliminating the records manager from the ATIPP Act.

2. Maintain the role but significantly reduce the records manager's responsibilities.

To maintain the convenience to the public by having only one place to go to make an access to information request for any Yukon Public Body, the role of the records manager under the ATIPP Act should be modified such that the only role of the records manager is to receive the requests for access to information and forward them within a short, specified timeframe to the Yukon Public Body that has custody or control of the records requested. All the responsibilities in the ATIPP Act to respond openly, accurately and completely should rest solely with the Public Body who receives the request and all communication with the Applicant or third parties should be the responsibility of the Public Body.

Modifying the responsibilities as described above will eliminate the negative aspects created by the role of the records manager so long as the time periods between receipt of the request for access to information by the records manager and the Public Body's receipt of the request from the records manager are short and the process effectively managed. Any delay created in accessing information under this model would be minor.

If option one is selected, Yukon Public Bodies will need to be given the authority to transfer a request for access to information received to another Yukon Public Body where appropriate. If either option is selected, how to manage time extension authorizations will require consideration. Some access to information laws authorize a Public Body to extend the time if certain circumstances exist with Commissioner oversight while others require approval of the Information and Privacy Commissioner.[129]

[128] "Custodian" in the HIPMA is defined to include: the Department [of Health and Social Services], a hospital operator or health facility, a health care provider [which includes a: medical practitioner; registered nurse or practitioner; licensed practical nurse; pharmacist; chiropractor; optometrist; dentist; dental assistant, therapist or hygienist, and denturist], prescribed Yukon First Nation program, and the Minister [of Health and Social Services].

[129] The head of a Public Body may extend the time for responding to a request for up to 30 days and for a longer period with the permission of the Commissioner for specified reasons in BC, AB, MB, NB, NS, and PEI. In SK and ON the head of a public body may only extend for 30 days. There is no option for a longer period with permission of the Commissioner. In Northwest Territories (NWT) and NU a head of a public body may extend the time for

SCOPE OF THE ATIPP ACT

As previously noted, a "public body" is defined in the ATIPP Act as:

> *(a) each department, secretariat, or other similar executive agency of the Government of Yukon; and*
>
> *(b) each body designated as a public body in a regulation made under section 68*

Yukon Public Bodies designed in *The Designation of Public Bodies Regulation* (Designation Regulation) are:

- *Child and Youth Advocate;*
- *A Designated Agency under the Adult Protection and Decision Making Act;*
- *First Nation service authority designated under the Child and Family Services Act;*
- *Yukon College;*
- *Yukon Development Corporation;*
- *Yukon Energy Corporation;*
- *Yukon Hospital Corporation (including hospitals and other facilities maintained or operated by the Yukon Hospital Corporation);*
- *Yukon Housing Corporation;*
- *Yukon Liquor Corporation;*
- *Yukon Lottery Commission;*
- *Workers' Compensation Health and Safety Board; and*
- *each board, commission, foundation, corporation or other similar agency established or incorporated as an agent of the Government of Yukon.*

The definition of "public body" in the ATIPP Act does not include municipalities.

Municipalities, like Yukon Public Bodies, are government bodies. Therefore, the same rationale that applies for providing a right of access to records in the custody or control of Yukon Public Bodies, applies to municipalities in Yukon. Also, like Yukon Public Bodies, municipalities collect, use and disclose

---

responding for a reasonable period for specified reasons. In NL a head of a public body must always apply to the Commissioner to extend the time for responding to the request.

personal information without any requirements to protect the privacy of the individuals whose personal information they are collecting.

When *Bill 80, Act to Amend the Access to Information and Protection of Privacy Act and the Health Act* was debated in the fall of 2009, the following comments were made regarding bringing municipalities within the scope of the ATIPP Act.

> *…municipalities are a form of public government and, hence, the information they hold about members of the public should be protected…and…there should be access to information provided…*[130]

> *… eventually [city councils] will be part and parcel of the ATIPP process. We just want to get more consultation done so that they're more comfortable with it…consultation is being done and will be done over the next 18 months.*[131]

> *….over the next 18 months, hopefully the municipalities will buy in to go forward with ATIPP, but this is a big decision for them to put their head around, per se, in how they would address it at that level. We're working with them and putting things together so, in the next 18 months, they'll be more comfortable with any decision that comes from that.*[132]

Six years has passed since these comments were made and municipalities are still not subject to the ATIPP Act. Consequently, the public has no right to access information held by municipalities and no assurance their privacy is being adequately protected.

As previously mentioned, the access and privacy landscape in Yukon has changed with the enactment of the HIPMA. Once HIPMA is proclaimed, custodians of all sizes will be required to comply. As a result, there is no further justification for excluding municipalities from application of the ATIPP Act. Most jurisdictions in Canada have access and privacy laws that are applicable to municipalities. To ensure Yukoners are afforded these same rights, the following is recommended.

Recommendation #12
Yukon municipalities should be made subject to the ATIPP Act.

During the 2009 debate in the Legislative Assembly, there was also discussion around the need to clarify what Yukon Public Bodies are included in the definition of "each board, commission, foundation, corporation or other similar agency established or incorporated as an agent of the Government of Yukon" contained in the Designation Regulation.

---

[130] Mr. Cardiff, former MLA, Fall Sitting, Yukon Legislative Assembly, 32nd Legislature, Hansard, November 5, 2009, p. 4909.

[131] Honourable Mr. Hart, former MLA, Fall Sitting, Yukon Legislative Assembly, 32nd Legislature, Hansard, December 14, 2009, p.5458.

[132] *Ibid.* 131.

As of March, 2006 there were 99 boards or committees listed in the Yukon Government Boards & Committees Directory.[133] There are currently 28 each of school boards and councils.

Not clarifying who these bodies are presents a number of risks. There are risks to a body that fits within the definition of a "public body" if they are not applying the ATIPP Act. There are also risks to the public if the body is not complying with the privacy requirements in Part 3 of the ATIPP Act. Also, by not clarifying the status of these bodies, the public is being essentially denied their right of access to information in the custody or control of these bodies given the public is unaware of their right to access this information.

To ensure Yukoners are not denied their rights under the ATIPP Act and to prevent non-compliance with the ATIPP Act by a Yukon Public Body, the following is recommended.

Recommendation #13

The boards, commissions, foundations, corporations or other similar agencies that are public bodies under the ATIPP Act should be specified in the Designation Regulation.

ADDITIONAL ATIPP ACT AMENDMENTS

Following are additional amendments to the ATIPP Act that should be considered. Most of the comments made below stem from NL's ATIPPA Review Report released following the recent comprehensive review of NL's ATIPPA conducted by NL's ATIPPA Review Committee. The ATIPP Act is similar to NL's ATIPPA and therefore the comments and recommendations made in the NL's ATIPPA Review Report are relevant.

Amendments Re: Role of ATIPP Coordinators

In the NL's ATIPPA Review Report, NL's ATIPPA Review Committee made the following observations about the role of ATIPP Coordinators in NL's Public Bodies:

> *Coordinators are not accorded the status and respect they should have, bearing in mind their central place in the fair and efficient treatment of the requests for information.*
>
> *…their work is often combined with other tasks. This may be because of relatively few requests within some public bodies. But it may also be due to an undervaluation of the role of treating requests as compared to other work.*

[133] Yukon Government Boards & Committees Directors, March 2006, Executive Council Office, located at www.eco.gov.yk.ca.

> *Some of the current delays in administering the ATIPPA may be due to the fact that most coordinators must juggle several tasks.*[134]
>
> *This relaxed approach to assigning ATIPPA responsibilities was mirrored in the lack of emphasis on training and the acquisition of professional qualifications*
>
> *Overall, the knowledge of ATIPP coordinators appears to be undervalued, and their autonomy to apply the law to the requests is limited by both their superiors and the minister's political staff. There is no more telling indication of the control exercised over the administration of the ATIPP system than the fact that the final communication with the requester, either to send the information or to explain the reasons for the refusal, comes, in the case of government departments, from the deputy minister's office and is signed by the deputy minister.*

NL's ATIPPA Review Report goes on to describe the level of positions ATIPP Coordinators generally hold within the Government of NL noting they are primarily low level positions. NL's ATIPPA Review Report also described the challenges faced by ATIPP Coordinators when trying to respond to an access to information request, such as the requirement to consult with and take direction from a number of individuals, including Deputy Ministers and communications staff, when processing these requests. On this point NL's ATIPPA Review Committee stated that:

> *This type of involvement by staff impairs the fair operation of the access to information system. It suggests the motivation for this involvement has much to do with the image of the government of the day in news coverage. Nowhere in the ATIPPA is it stated that a valid reason for withholding information is how the government might be affected by media coverage of information disclosed through the Act*
>
> *… the time spent on certain categories of requesters perceived as problematic through prior identification adds to delays and negates the duty to assist.*
>
> *…the current system, where requests are scrutinized by staff, the deputy minister, and often the minister, facilitates the interpretation of ATIPPA in a partisan political way rather than in a fair, principled way.*[135]

The following was recommended by NL's ATIPPA Review Committee to remedy the problems identified.

1. *The Act be amended to give delegated authority for handling a request solely to the ATIPP coordinator.*
2. *No officials other than the ATIPP coordinator be involved in the request unless they are consulted for advice in connection with the matter or giving assistance in obtaining and locating the information.*

---

[134] *Ibid.* 89, p. 45.

[135] *Ibid.* 89, p. 46.

3. *The Act be amended to anonymize the identity and type of requester upon receipt of the request and until the final response is sent to the requester by the ATIPP coordinator, except where the request is for personal information or the identity of the requester is necessary to respond to the request.*

The problems described above by NL's ATIPPA Review Committee for NL's Public Body' ATIPP Coordinators are the same for the ATIPP Coordinators in Yukon Public Bodies. To ensure access to information rights are not being negatively impacted due to assigning of the ATIPP Coordinator role and management of access to information requests within Yukon Public Bodies, the following is recommended.

Recommendation #14
The ATIPP Act should be amended to ensure that:

- **ATIPP Coordinators in each Yukon Public Body are given sole delegated authority to handle requests for access to information;**
- **no officials in Yukon Public Bodies other than the ATIPP coordinator are involved in the request unless they are consulted for advice in connection with the matter or giving assistance in obtaining and locating the information; and**
- **the identity and type of requester remains anonymous until the final response is sent to the requester by the ATIPP coordinator, except for requests made for personal information or the requests where the identity of the requester is necessary to respond to the request.**

Given the complex nature of interpreting and applying the ATIPP Act when receiving an access to information request, the following is also recommended.

Recommendation #15
Consideration should be given to requiring that ATIPP Coordinators be positioned at least a management level within Yukon Public Bodies and be provided adequate training about how to interpret and apply the ATIPP Act to ensure the provisions under Part 2 of the ATIPP Act are properly applied.

Amendments Re: Public Interest Override

In NL's ATIPPA Review Report, NL's ATIPPA Review Committee made the following comments about the meaning of a public interest override in access to information and protection of privacy laws.

> *The public interest override in access laws recognizes that even when information fits into a category that deserves protection, there may be an overriding public interest in disclosing it to an applicant or to the public at large. In that respect, the public interest test is a kind of lens that public officials must look through in order to make a final determination about disclosure. The United Kingdom Information Commissioner's Office argues that, by necessity, the public interest should be broadly focused:*

> *The public interest can cover a wide range of values and principles relating to the public good, or what is in the best interests of society. For example, there is a public interest in transparency and accountability, to promote public understanding and to safeguard democratic processes*.

> *The public interest override in the ATIPPA and most other Canadian access laws typically applies to public health and safety and the environment, and is conditional on the risk of harm being significant, or on the presence of a compelling public interest. By contrast, the public interest override in access laws in the United Kingdom, New Zealand, and some of the Australian states covers more topics and is less restrictive in its application.*[136]

After reviewing the legal landscape nationally and internationally and noting the narrowness of the NL's ATIPPA subsection 31 (1), which is same as section 22 of the ATIPP Act, NL's ATIPPA Review Committee concluded the following.

> *The approach to the public interest override in the ATIPPA is in need of an overhaul. It applies to few areas of public interest, and the wording suggests it is intended mainly for urgent matters. The existing section 31(1) is useful for the purpose for which it is intended, where it places a positive duty on the head of a public body to release information related to a risk of significant harm to the environment or to public health and safety even in the absence of a request for the information. The Committee concludes that in a modern law and one that reflects leading practices in Canada and internationally, it is necessary to broaden the public interest override and have it apply to most discretionary exemptions. This would require officials to balance the potential for harm associated with releasing information on an access request against the public interest in preserving fundamental democratic and political values. These include values such as good governance, including transparency and accountability; the health of the democratic process; the upholding of justice; ensuring the honesty of public officials; general good decision making by public officials. Restricting the public interest to the current narrow list implies that these other matters are less important.*[137]

With respect to including a public interest override provision in NL's ATIPPA, NL's ATIPPA Review Committee made the following recommendations.

1. *With respect to disclosure in the public interest:*

   (a) *The provisions of section 31(1) be retained; and*

   (b) *The Act also provide that where the head of a public body may refuse to disclose information to an applicant under one of the following discretionary exceptions in Part III of the Act, that discretionary exception shall not apply where it is clearly demonstrated that the public interest in disclosure outweighs the reason for the exception:*

[136] *Ibid*. 89, p. 67.

[137] *Ibid*. 89, p. 78.

- *section 19 (local public body confidences)*
- *section 20 (policy advice or recommendations)*
- *section 21 (legal advice)*
- *section 22.1 (confidential evaluations)*
- *section 23 (disclosure harmful to intergovernmental relations or negotiations)*
- *section 24 (disclosure harmful to the financial or economic interests of a public body)*
- *section 25 (disclosure harmful to conservation)*
- *section 26.1 (disclosure harmful to labour relations interest of public body as employer)*[138]

2. *NL's Office of the IPC provide training for NL's Public Bodies, as well as general guidance manuals on the public interest test, including how it is to be applied.*

For the reasons noted by NL's ATIPPA Review Committee above and those set out in the letter dated April 3, 2014 addressed to the Honourable Wade Istchenko, then Minister of Highways and Public Works (attached), the following is recommended.

Recommendation #16
A public interest override provision similar to that recommended by NL's ATIPPA Review Committee should be included Part 2 of the ATIPP Act.

Amendments Re: Ministerial Briefing Records

NL's ATIPPA Review Committee examined the amendments made to NL's ATIPPA in 2012 that resulted in a full exclusion from NL's ATIPPA access to ministerial briefing records under subsections 7 (4), (5) and (6) which stated:

> *(4) The right of access does not extend*
>
> *(a) to a record created solely for the purpose of briefing a member of the Executive Council with respect to assuming responsibility for a department, secretariat or agency; or*
>
> *(b) to a record created solely for the purpose of briefing a member of the Executive Council in preparation for a sitting of the House of Assembly.*
>
> *(5) Paragraph (4)(a) does not apply to a record described in that paragraph if 5 years or more have elapsed since the member of the Executive Council was appointed as the minister responsible for the department, secretariat or agency.*

[138] *Ibid*. 89, p. 79.

(6) Paragraph (4)(b) does not apply to a record described in that paragraph if 5 years or more has elapsed since the beginning of the sitting with respect to which the record was prepared.

NL's ATIPPA Review Committee noted the following about the reasons for the amendment.

- There are two categories of information in ministerial briefing records: subject areas and issues that a minister needs to be aware of, and policy advice and recommendations on those matters.[139]
- Prior to the amendments ATIPP Coordinators would do a line by line review and redact policy advice.[140]
- No ministerial briefing records had been released since the amendments although seven requests for access were received whereas prior to the amendments three quarters of 48 requests resulted in partial disclosure.[141]
- The Cummings report, which precipitated the amendments, highlighted the need to protect advice and recommendations in ministerial briefing records but did not recommend that "ministers briefing books be protected as a separate category of records."[142]

Upon reviewing access laws in Canada, NL's ATIPPA Review Committee noted that:

- the provisions included in NL's ATIPPA were modeled after AB's FOIP Act.[143]
- Yukon has similar provisions and is the only jurisdiction in Canada that protects information used for briefing the Premier;[144]
- PEI does not allow access to records "by or for a member of the Executive Council, or a member of the Legislative Assembly; and[145]
- None of the remaining provinces or territories has similar provisions.[146]

---

[139] *Ibid*. 89, p. 79.

[140] *Ibid*. 89, p. 79.

[141] *Ibid*. 89, p. 80.

[142] *Ibid*. 89, p. 82.

[143] *Ibid*. 89, p. 83.

[144] *Ibid*. 89, p. 83.

[145] *Ibid*. 89, p. 83.

[146] *Ibid*. 89, p. 83.

In evaluating whether to maintain the exemption, NL's ATIPPA Review Committee concluded that:

- There is sufficient protection within NL's ATIPP Act to protect policy advice and recommendations, namely under sections 18 (Cabinet Confidences), 20 (policy advice and recommendations), section 23 (intergovernmental relations or negotiations), 24 (financial or economic interests of a public body), and 26.1 (labour relations interests of a public body as employer).[147]

- The recent decision by the Supreme Court of Canada in *John Doe v. Ontario (Finance) 2014 SCC 36*[148] reinforces that the authority to refuse disclosure where disclosure would reveal advice or recommendations and includes policy options.[149]

These conclusions, together with the recognition of the importance of protecting policy advice and recommendations in the functioning of government and after confirming the ability to separate policy advice and recommendations in briefing records from factual material, NL's ATIPPA Review Committee recommended the following.

- *Sections 7(4),(5), and (6) of the Act, respecting briefing books prepared for ministers assuming responsibility for a new department or to prepare for a sitting of the House of Assembly, be repealed.*

- *Public bodies change the manner in which briefing books are assembled, so that policy advice and Cabinet confidences are easily separable from factual information.*

As was noted by NL's ATIPPA Review Committee, the ATIPP Act contains a similar exemption to the right of access to ministerial briefing records as did NL's ATIPPA, which is set out in subsections 5 (4) and (5).

> *5 (4) The right of access to a record does not extend to a record created solely for the purpose of*
>
> > *(a) briefing a Minister in respect of assuming responsibilities under the Government Organisation Act for a department or corporation;*
> >
> > *(b) briefing a Minister in relation to a sitting of the Legislative Assembly, including briefings prepared to support the Minister for debate of an appropriation bill; and*
> >
> > *(c) briefing the Premier in respect of forming a new government*
>
> *5 (5) Subsection 4 does not apply*

[147] *Ibid*. 89, pp. 80 and 83.

[148] In John Doe, the Supreme Court of Canada held that the reference to advice and recommendations in the Ontario FIPPA legislation would include polity options.

[149] *Ibid*. 89, pp. 80 and 83.

(a) to a record described in paragraph 4(a), if five or more years have passed since the Minister was appointed as the Minister responsible for the department or corporation;

(b) to a record described in paragraph 4(b), if five or more years have passed since the beginning of the sitting in respect of which the record was created; and

(c) to a record described in paragraph 4(c), if five or more years have passed since the date on which the new government was formed.

The ATIPP Act has similar provisions to those identified by NL's ATIPPA Review Committee which provide sufficient protection for policy advice and recommendations contained in ministerial briefing records, namely: sections 15 (Cabinet confidences), 16 (policy advice, recommendations and draft regulations), 17 (disclosure harmful to the financial or economic interests of a public body), and 20 (disclosure harmful to intergovernmental relations or negotiations). Based on the analysis done by NL's ATIPPA Review Committee, these sections together with the John Doe case[150] should be sufficient authority in the ATIPP Act to protect the confidentiality of policy advice and recommendations contained in ministerial briefing records. Consequently, in line with the purposes of the ATIPP Act to give the public the right of access to information, the following is recommended.

Recommendation #17
Subsections 5 (4) and (5) of the ATIPP Act should be repealed.

In accordance with the second recommendation made by NL's ATIPPA Review Committee in respect of ministerial briefing records, to provide further protection to the policy advice and recommendations in these records, the following is also recommended.

Recommendation #18
Consideration should be given to implementing a policy or process that requires Yukon Public Bodies to change the manner in which ministerial briefing records are assembled so that policy advice, recommendations and other Cabinet confidences are easily separable from factual information.

Amendments Re: Legislative Paramountcies

NL's ATIPPA Review Committee examined all provisions in NL's laws that were paramount over NL's ATIPPA to determine whether the paramountcy should remain. Following its review, it determined that some should not remain. At the conclusion of the examination, it recommended, *inter alia*, that every statutory five-year review of NL's ATIPPA should include a review of each legislative provision that is paramount over NL's ATIPPA.

In Yukon, there are several provisions in legislation and some entire Acts that are paramount over the ATIPP Act making information inaccessible to the public through the ATIPP Act and removing some of the privacy protections. Given this, the following is recommended.

[150] Paragraph 15 (1)(b) in our ATIPP Act provides an express exception for records containing policy options.

Recommendation #19

Section 69 of the ATIPP Act should be amended to include a requirement that any provisions in a Yukon law that is paramount over the provisions in the ATIPP Act are reviewed each six years during the comprehensive review of the ATIPP Act to evaluate whether these paramountcies are necessary.

Amendments by Section

Section 1 (Purposes of this Act)

Recommendation #20

Section 1 of the ATIPP Act should be evaluated to ensure the purposes are still accurately reflected given the shift from paper to electronic information management and greater emphasis on accountability.

See section 3 of NL's ATIPPA as an example.

Section 2 (Scope of this Act)

NL's ATIPPA Review Committee recommended that NL's Commissioner be given express authority to require production of records relating to disputes regarding the following records to determine whether those records fall within NL's IPC's jurisdiction under NL's ATIPPA.

> *(g) a record of a question that is to be used on an examination or test;*
>
> *(i) material placed in the custody of the Provincial Archives of Newfoundland and Labrador by or for a person, agency or organization other than a public body;*
>
> *(j) material placed in the archives of a public body by or for a person, agency or other organization other than the public body;*[151]

Paragraphs 2 (1)(d), (e) and (g) of the ATIPP Act are similar to these paragraphs. As such, the following is recommended.

Recommendation #21

The IPC should be granted authority in Part 4 of the ATIPP Act to require production of records relating to disputes about whether a request for access to records involves those records described in paragraphs 2 (1)(d), (e) and (g) of the ATIPP Act.

Section 3 (Definitions)

Recommendation #22

The terms "applicant", "complaint", "review", "request" and "third party" should be defined in section 3 of the ATIPP Act. See NL's ATIPPA for wording.

[151] *Ibid*. 89, p. 136.

Section 4 (Parmountcy of this Act)

Recommendation #23
The relationship of the ATIPP Act with the HIPMA should be specified in section 4 of the ATIPP Act.

Section 16 (Policy advice, recommendations or draft regulations)

NL's ATIPPA Review Committee recommended repealing paragraph 20 (1)(c) of NL's ATIPPA after determining there is adequate protection for consultations and deliberations under paragraph 20 (1)(a). These paragraphs follow.

> *20. (1) The head of a public body may refuse to disclose to an applicant information that would reveal*
>
> > (a) advice, proposals, recommendations, analyses or policy options developed by or for a public body or minister;
> >
> > *(c) consultations or deliberations involving officers or employees of a public body, a minister or the staff of a minister;*[152]

Section 16 in the ATIPP Act contains similar provisions.

> *16(1) A public body may refuse to disclose information to an applicant if the disclosure would reveal*
>
> *(a) advice, proposals, recommendations, analyses or policy options developed by or for a public body or a Minister;*
>
> *(b) consultations or deliberations involving officers or employees of a public body or a Minister relating to the making of government decisions or the formulation of government policy;*

Given the similarities between these paragraphs and those in NL's ATIPPA, the following is recommended.

Recommendation #24
Paragraph 16 (1)(b) in the ATIPP Act should be repealed.

Section 23 (Information that will be published or released within 90 days)

Recommendation #25
The term "published" in section 23 of the ATIPP Act should be defined.

Section 26 (Notifying the third party)

Subsection 26 (1) of the ATIPP Act states the following:

[152] *Ibid*. 89, p. 109.

26 (1) Before giving access to records that a public body believes may contain information to which section 24 [disclosure harmful to a third party's business interests] or 25 [disclosure harmful to a third party's personal privacy] applies, the records manager must, if practicable, give the third party notice.

The way this provision is applied by Yukon Public Bodies is that they notify third parties if they determine there is third party personal or business information in the record before any decision is made about whether a record does or does not contain this information. The result is that delays are caused in providing access while third party notifications occur.

In a recent Supreme Court of Canada decision, the majority stated the following about the duty to notify a third party business under Canada's *Access to Information Act* (AIA).

The Act…establishes a process of notification…This process permits the third party to mount objections and have them considered before the information is disclosed. Section 27(1) of the Act details the circumstances in which a government institution must make every reasonable effort to give notice of its intention to disclose the third party's information.[153]

27. (1) Where the head of a government institution intends to disclose any record requested under this Act, or any part thereof, that contains or that the head of the institution has reason to believe might contain

(a) trade secrets of a third party,

(b) information described in paragraph 20(1)(b) that was supplied by a third party, or

(c) information the disclosure of which the head of the institution could reasonably foresee might effect a result described in paragraph 20(1)(c) or (d) in respect of a third party,

the head of the institution shall, subject to subsection (2), if the third party can reasonably be located, within thirty days after the request is received, give written notice to the third party of the request and of the fact that the head of the institution intends to disclose the record or part thereof.

In this case, the appellant argued that subsection 27 (1) required that the public body automatically notify a third part if a record contains third party business information. The court rejected the argument. Cromwell J. writing for the majority stated "…I do not accept Merck's submission that there is any "automatic" right to notice with respect to certain categories of records. Such a right to

[153] Para. 27.

automatic notice is not supported by the text or purpose of the provisions or by the jurisprudence that has interpreted them."[154] He then clarified how the notice provisions in the AIA work.

> *The institutional head has a general duty, subject to the other provisions of the Act, to provide access to the record requested (s. 4(1))…The notice provisions relate to how the institutional head carries out that duty.*
>
> *In considering a request for disclosure of third party information under the Act, the institutional head has four main possible courses of action (aside from the exercise of discretion under s. 20(6)), two of which engage the notice provisions. He or she may decide to (i) disclose the requested information without notice; (ii) refuse disclosure without notice; (iii) form an intention to disclose severed material with notice; or (iv) give notice because there is reason to believe that the record requested might contain exempted material.*[155]
>
> … in order to disclose third party information without giving notice, the head must have no reason to believe that the information might fall within the exemptions under s. 20(1). Conversely, in order to refuse disclosure without notice, the head must have no reason to believe that the record could be subject to disclosure. If the information does not fall within one of these clear categories, notice must be given. I would therefore interpret the phrase "intends to disclose" as referring to situations which fall between those in which the head concludes that neither disclosure nor refusal of disclosure without notice is required. In other words, the head "intends to disclose" a record "that the head . . . has reason to believe might contain" exempted information unless the head concludes either (a) that there is no reason to believe that it might contain exempted information (in which case disclosure without notice is required) or (b) that he or she has no reason to believe that disclosure could be required by the Act (in which case refusal of disclosure without notice is required).[156]

In order to reduce time delays caused by unnecessary third party notifications under the ATIPP Act, the following is recommended.

Recommendation #26

Consideration should be given to developing a process to guide ATIPP Coordinators on the application of section 26 to reduce delays in providing access to information caused by unnecessary third party notifications.

The records manager has in the past interpreted section 26 to operate outside the timelines in subsection 11 (1) of the ATIPP Act, which it does not. Placing the timelines associated with third party notification in the sections dealing with a response to a request for access to information near the beginning of Part 2 in the ATIPP Act is one way this confusion can be resolved. The wording in section

[154] Para. 63.

[155] Para. 71.

[156] Para. 77.

19 below that was added to NL's ATIPPA when it was amended is useful. This section also addresses the problem of releasing the records at the expiry of a third party's deadline for response without knowledge of whether the third party has requested a review of the public body's decision to release the records.

Third party notification

19. (1) Where the head of a public body intends to grant access to a record or part of a record that the head has reason to believe contains information that might be excepted from disclosure under section 39 or 40, the head shall make every reasonable effort to notify the third party.

(2) The time to notify a third party does not suspend the period of time referred to in subsection 16 (1).

(3) The head of the public body may provide or describe to the third party the content of the record or part of the record for which access is requested.

(4) The third party may consent to the disclosure of the record or part of the record.

(5) Where the head of a public body decides to grant access to a record or part of a record and the third party does not consent to the disclosure, the head shall inform the third party in writing

(a) of the reasons for the decision and the provision of this Act on which the decision is based;

(b) of the content of the record or part of the record for which access is to be given;

(c) that the applicant will be given access to the record or part of the record unless the third party, not later than 15 business days after the head of the public body informs the third party of this decision, files a complaint with the commissioner under section 42 or appeals directly to the Trial Division under section 53 ; and

(d) how to file a complaint or pursue an appeal.

(6) Where the head of a public body decides to grant access and the third party does not consent to the disclosure, the head shall, in a final response to an applicant, state that the applicant will be given access to the record or part of the record on the completion of the period of 15 business days referred to in subsection (5), unless a third party files a complaint with the commissioner under section 42 or appeals directly to the Trial Division under section 53 .

(7) The head of the public body shall not give access to the record or part of the record until

(a) he or she receives confirmation from the third party or the commissioner that the third party has exhausted any recourse under this Act or has decided not to file a complaint or commence an appeal; or

(b) a court order has been issued confirming the decision of the public body.

(8) The head of the public body shall advise the applicant as to the status of a complaint filed or an appeal commenced by the third party.

To address the problems identified above, the following is recommended.

Recommendation #27

Section 26 of the ATIPP Act should be repealed and a new section 11.1 added following section 11 that is similar to the third party notification provisions in section 19 of NL's ATIPPA.

Section 32 (Right to request correction of personal information)

Section 32 of the ATIPP Act states the following.

32*(1) A person who believes there is an error or omission in the person's personal information may request the records manager to request the public body that has the information in its custody or under its control to correct the information.*

(2) If no correction is made in response to a request under subsection (1), the public body must annotate the record with the correction that was requested but not made.

(3) If personal information is corrected or annotated under this section, the public body must give notice of the correction or annotation to any public body or any third party to whom that information has been disclosed during the year before the correction was requested.

(4) On being notified under subsection (3) of a correction or annotation of personal information, a public body must make the correction or annotation on any record of that information in its custody or under its control.

For the reasons previously mentioned, the responsibilities of records manager should either be removed from this section or the responsibility of the records manager limited to receiving and passing on the request for correction to the appropriate the public body.

There are no timelines in the ATIPP Act for responding to a request for correction. Timelines to respond to a correction were added to NL's ATIPPA during the recent amendments.

Time limit for final response

16. (1) The head of a public body shall respond to a request in accordance with section 17 [Content of final response for access] *or 18* [Content of final response for correction of personal information]*, without delay and in any event not more than 20 business days after receiving it, unless the time limit for responding is extended under section 23.*

(2) Where the head of a public body fails to respond within the period of 20 business days or an extended period, the head is considered to have refused access to the record or refused the request for correction of personal information.

The following is recommended to ensure corrections requests are responded to by a Yukon Public Body in a timely manner.

Recommendation #28
Timelines to process a request for correction should be included in the ATIPP Act.

Consideration should be given to structuring all the duties of a public body associated with processing a request for access, including for managing third party notifications, and a request for correction together in Yukon's ATIPP Act similar to NL's ATIPPA, Part II, Access and Correction.[157]

Section 34 (Retention of Personal Information)

Recommendation #29
Section 34 of the ATIPP Act should be amended to add a requirement that upon receipt by a Yukon Public Body of a request for personal information or to correct personal information from an individual, the Public Body must retain the information for as long as necessary to allow the individual to exhaust any recourse under the ATIPP Act that he or she may have with respect to the request.

See subsection 65 (2) of NL's ATIPPA as an example.

Section 36 (Disclosure of Personal Information)

Recommendation #30
Section 36 of the ATIPP Act should authorize a Yukon Public Body to disclose personal information to an individual if the request is made by the individual for his or her own personal information.

This will allow an individual to have access to their own personal information without having to go through the formal process. See paragraph 57 (1)(a) of the HIPMA for an example.

Part 4 (Office and Functions of Information and Privacy Commissioner)

Recommendation #31
The IPC should be authorized under Part 4 to discontinue an investigation or review in certain circumstances.

See section 101 of the HIPMA for circumstances that authority the IPC under that Act to discontinue an investigation into a complaint.

Section 46 (Delegation by Commissioner)

[157] This Part contains the following provisions: Right of access (section 8), Public interest (section 9), Right to request correction of personal information (section 10), Making a request (section 11), Anonymity (section 12), Duty to assist applicant (section 13), Transferring a request (section 14), Advisory response (15), Time limit for final response (section 16), Content of final response for access (section 17), Content of final response for correction of personal information (section 18), Third party notification (section 19), Provision of information (section 20), Disregarding a request (section 21), Published material (section 22), Extension of time limit (section 23), Extraordinary circumstances (section 24), Costs (section 25), and Estimate and waiver of costs (section 26).

Recommendation #32

The IPC should be authorized under section 46 to delegate any duty or power under the ATIPP Act, including for conducting reviews.

Section 54 (Burden of Proof)

As was noted by the Yukon Supreme Court in *Branigan v. Commissioner of the Yukon Territory*, 2004 YKSC 79 (CanLII)[158], the burden of proof under 54 (2)(a) is a challenge to meet when the person who must discharge the burden does not know the content of the information. As a result, the following is recommended.

Recommendation #33

Paragraph 54 (2)(a) of the ATIPP Act should be amended to place the burden of proof where personal information is at issue in a review on the public body to prove that the disclosure of the information would not be contrary to the ATIPP Act.

See subsection 43 (2) of NL's ATIPPA as an example.

Section 67 (Offences and penalties)

Given the new risks to personal information as stated above the offence provisions of the ATIPP Act should be amended as follows.

Recommendation #34

Section 67 of the ATIPP Act should be repealed and replaced with the following.

> ***67 (1) A person who knowingly collects, uses or discloses personal information in contravention of this Act or the regulations is guilty of an offence and liable, on summary conviction, to a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.***
>
> ***(2) A person who knowingly***
>
> ***(a) attempts to gain or gains access to personal information in contravention of this Act or the regulations;***
>
> ***(b) makes a false statement to, or misleads or attempts to mislead the commissioner or another person performing duties or exercising powers under this Act;***
>
> ***(c) obstructs the commissioner or another person performing duties or exercising powers under this Act;***
>
> ***(d) destroys a record or erases information in a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records; or***

[158] Paras. 32 to 34.

(e) alters, falsifies or conceals a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records,

is guilty of an offence and liable, on summary conviction, to a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.

(3) A prosecution for an offence under this Act shall be commenced within 2 years of the date of the discovery of the offence. [159]

Section 68 (Power to make regulations)

Recommendation #35

Section 68 should be amended to authorize the Commissioner in Executive Council to make a regulation authorizing the waiving of fees to process a request for access to information if disclosure of the record is in the public interest.

[159] This is similar to the section 115 in NL's ATIPPA.