

IPC Access & privacy matters

2014 Annual Report of the Yukon Information & Privacy Commissioner



Management of personal information must be made a priority in an increasingly digitized environment.

Improving compliance, improving performance

I am pleased to provide my second Annual Report as Information and Privacy Commissioner.

Our focus in 2014 has been on improving compliance with the *Access to Information and Protection of Privacy Act* (ATIPP Act) and on our performance.

Managing access and privacy is of national concern

In 2014 Information and Privacy Commissioners (IPCs) across Canada issued a joint resolution that noted the following.

- Digital information is the lifeblood of government. It is the foundation of decision-making, policy development, and service delivery to citizens.
- Unprecedented volumes of information must be organized, stored, searched and secured to facilitate access and protect privacy. Technologies are changing the nature of government records and challenging traditional information practices.
- Privacy rights are being eroded by technological developments which increase the risk of over-collection, over-retention, inappropriate sharing, data matching, and breaches.
- The use of technology has increased 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.

The IPCs committed to following up with public bodies to ensure they are:

- embedding privacy and access rights into the design of programs and systems;
- adopting administrative and technological safeguards to prevent loss or destruction of records, storing and retaining records as required and for ease of retrieval, mitigating the risks of privacy breaches and limiting the collecting and sharing of personal information strictly as necessary to meet program or activity objectives;
- establishing clear accountability mechanisms for managing information throughout its lifecycle, from collection to disposition or destruction;
- ensuring all employees are trained in how to properly manage information, digital or otherwise, including on their obligation to protect privacy and access rights; and
- moving towards making information more accessible to citizens in accordance with open government principles.

Yukoners' privacy a priority

In line with the commitment in the joint resolution, I have been working proactively with public bodies in 2014 to promote compliance with the ATIPP Act. Workshops were offered, the submission of privacy impact assessments (PIAs) encouraged and recommendations made to mitigate risks to privacy. In addition, publications were issued to increase awareness about the requirements of the ATIPP Act, and meetings were held with various groups to discuss these requirements.

This year I consistently conveyed the need for public bodies to have a privacy management program. In late 2014 I met with senior officials of public bodies and informed them I plan to evaluate the maturity of their privacy management programs in 2015 and will report on the status in future annual reports. In early 2015 two workshops were offered: how to develop a privacy management program and how to complete a PIA.

Yukon has its own unique challenges to consider when evaluating the ability of Yukon public bodies to manage their access and privacy responsibilities. Yukoners should not accept these challenges as a reason for less access to information and privacy protection than citizens in other parts of Canada. Yukon public bodies have a significant amount of work to do to ensure Yukoners' personal information is adequately protected. Privacy management must be made a priority if public bodies intend on using technology for service delivery. The implementation of several electronic information systems in 2014, including two that contain Yukoners' highly sensitive health information, suggests the time has come for making privacy protection a high priority.

ATIPP Act review in 2015

A full review of the ATIPP Act is scheduled for 2015. Now 20 years old, the Act requires updating given the shift from the use of paper records to the use of technology.

A comprehensive review of the ATIPP Act should occur to enable use of technology for business while ensuring access and privacy rights are adequately protected. Most jurisdictions in Canada are carrying out a review of their access and privacy legislation with the ubiquitous use of technology in mind and I strongly encourage Yukon government to do the same.

Update on goals

In my 2013 Annual Report I set out three goals: build relationships with public bodies to improve compliance with the ATIPP Act; improve the performance of my office; and

demonstrate accountability both of my office and of public bodies.

In my prior comments I discussed the activities undertaken by the office towards the first goal.

The office has been working diligently on the second goal. To improve our performance, we have established a new Early Case Resolution (ECR) process designed to manage complaints and requests for reviews in a timely manner. There are now two teams in the office.

The ECR Team will focus on working with complainants and public bodies to informally resolve complaints and requests for review.

The Investigation and Compliance Review Team, will focus on conducting full-fledged investigations where needed and providing feedback on PIAs and reported breaches.

I am confident that our new processes and structure will enable the office to more quickly resolve complaints and requests for review received under the ATIPP Act and complaints received under the *Ombudsman Act* and the *Public Interest Disclosure of Wrongdoing Act* and *Health Information Privacy and Management Act* once they are brought into force.

I reviewed our information management practices in 2014 and developed policies and procedures to strengthen the protection of information. I have also been working to improve our information security and to ensure personal information involved in service agreements is properly protected.

For the third goal, timelines have been established for the management of our case files that will be used to measure our performance each year. This information can be found on our statistics page along with other statistics about public bodies' interaction with our office.

I encourage Yukoners to read the stories that follow in this Annual Report and review the statistics to gain a better understanding of our work and how our work strengthens their access to information and privacy rights.

19th Annual Report

As required by the ATIPP Act, I am submitting this 19th Annual Report to the Honourable David Laxton, Speaker of the Yukon Legislative Assembly, who will in turn present it to that body.

Diane McLeod-McKay
Information and Privacy Commissioner

Contact us

Call	867-667-8468
Toll-free	1-800-661-0408 ext. 8468
Fax	867-667-8469
Email	info@ombudsman.yk.ca
Online	www.ombudsman.yk.ca
Address	201 – 211 Hawkins Street Whitehorse, Yukon Y1A 1X3

Case Summaries These stories are good examples of how our office helps public bodies, such as Yukon government departments, meet the requirements of the ATIPP Act.

Extensions after deadline not allowed

One inquiry undertaken in 2014 was on a request for review made by an individual who had requested access to records held by Community Services.

An issue that arose during the review was whether the records manager had authority to extend the deadline to respond to the request for access to records after the deadline had passed. It was found that the records manager did not have this authority. The result of extending without authority meant the extension was invalid and the public body was deemed to have refused the applicant access to the records for not having provided the applicant with a response by the deadline. The full Inquiry Report can be found on our website.





Our office is here to help you. Sometimes our role is simply to provide information and clarification. Other times we are working hard to protect your rights.

Thinkstock photo

Our involvement in privacy breach management improves privacy protection

A number of privacy breaches came to our attention in 2014. In one, a former employee of Education alleged his personal information collected through the security clearance process used by Education was collected, used, or disclosed contrary to the ATIPP Act.

We investigated the complaint and found the process was not in compliance with the ATIPP Act and that a privacy breach had occurred. Education acknowledged the problem and modified their process to ensure a privacy breach would not recur. The former employee was satisfied with the outcome and the matter was settled.

Education is working with our office to improve security clearance processes used across government.

We received two other breaches self-reported by public bodies. Public bodies who proactively report a breach to us obtain our assistance to more effectively manage the breach by ensuring the cause is identified and the risks of further breach addressed, the risk of harm to affected individuals is properly assessed and adequate notification provided, and changes are made to avoid another breach.

We do not report details associated with self-reported breaches to encourage continued reporting and ultimately better privacy protection for Yukoners.

No harm to business interests

This year, we saw an increase in the number of requests for review by businesses that provided information to a public body through the bid process and for which a request for access to the information was received by the public body.

The ATIPP Act allows a business to request the IPC review a decision by a public body to release third party business information. Businesses requesting a review of a public body's decision are often surprised to learn that under the ATIPP Act they have the burden of proving that a release of information will cause harm to their business interests. Of the requests for review we received from third party businesses, none were able to meet the three-part test required to establish harm would occur. The information was, therefore, released.

One of the purposes of the ATIPP Act is to make information held by public bodies accessible to the public in order to promote transparency in decision-making. When conducting business with public bodies, including Yukon government departments, businesses should be aware that any information provided is subject to the ATIPP Act and accessible to the public unless releasing the information would cause harm to a third party business interest.

In order to prevent unnecessary reviews by my office and to facilitate access to information, I encourage businesses to learn more about what constitutes harm to a business interest under the ATIPP Act. I also encourage them to inform public bodies about information provided that would be considered harmful to their business interest if released.



Meeting with the ATIPP Coordinators to improve access to information

Quick to resolve matters

Contact with our office is often from people seeking information. Some callers have concerns that we can resolve quickly with a simple phone call.

When a worried individual contacted us about not having received the records she requested, we were able to provide her the reason after contacting the records manager. The reason was she had not paid the fee owing for the records.

Some concerns cannot be resolved with a simple phone call. In such cases, we request a complaint or request for review

form be completed. We will then transfer the file to the ECR Team who will get to work on trying to settle the matter.

For example, we received a complaint from an individual about the disclosure of her personal information. Her personal information appeared on a licence that would be displayed publicly. The information was such that it could have caused her embarrassment or other harm. We requested the public body review their practice around disclosing personal information on licences to ensure they are meeting the requirements of the ATIPP Act.

This complaint was successfully resolved in less than 60 days.

Reasons must be given

In 2014 we issued one Investigation Report. It was determined that the individual who requested the information received a response to two requests for access to information without the information required by the ATIPP Act.

The ATIPP Act sets out what the records manager must include in a response. Missing from the response provided to the individual were the reasons why the public body severed information from the records released and the proper identification of the provisions relied on for the severing. The ATIPP Act requires both the provision and the reasons be included in a response to enable an applicant to evaluate whether the public body properly applied the ATIPP Act.

Our review of responses by the records manager indicates this information is not consistently provided. We will be monitoring responses to ensure this information is included.



Kudos to you

Shout out to **Health and Social Services** (HSS) for completing a PIA on its Panorama and Incident Management Reporting electronic information systems. The PIA for Panorama is one of the most complex I have ever seen and I commend HSS for its work on the PIA and for working collaboratively with my office through the process.

Shout out to **Yukon Hospital Corporation** (YHC) for completing a PIA on its Health Information System Connect project. This was a challenging piece of work and I commend YHC for its work on the PIA and for working collaboratively with my office.

Budget summary

This budget summary is for the fiscal year for the Information and Privacy Commissioner's (IPC's) Office which runs from April 1, 2014 to March 31, 2015. The prior fiscal year is shown for comparison purposes.

I have modified the way we report our budget to align with how the budget is allocated. The budget is allocated for operational expenses which include personnel and other. The "other" category includes things like rent, contract services, supplies, travel, and advertising.

The budget is also allocated for capital expenses which includes things like technology and furniture. Personnel and capital are reported jointly for both the Office of the Ombudsman and IPC. The "other" category is the budget allocated specifically for the operations of the IPC's Office or the Ombudsman's Office.

The increase in other budget allocation for the IPC's office in 2014/15 was due to the

expectation that the *Health Information Privacy and Management Act* would come into force. Much of the allocated budget for this was not spent but rolled into the 2015/16 budget.

The increase in capital budget for 2014 was allocated in order for the Offices to obtain a case management system to help us better manage our case files and perform our work more efficiently.

The process to acquire a case management system has taken longer than expected. Therefore, we were unable to purchase a case management system in 2014 and did not spend the money allocated, which was \$100,000. This money has been added to our 2015/16 budget as we anticipate being able to purchase the case management system in the next fiscal year. The small increase to the personnel budget was a cost-of-living increase for staff.

2013/14

Personnel (combined)	\$628,000
Other (IPC's office)	\$99,000
Other (Ombudsman's office)	\$97,000
Capital (combined)	\$2,000
Total	\$826,000

2014/15

Personnel (combined)	\$645,000
Other (IPC's office)	\$134,000
Other (Ombudsman's office)	\$81,000
Capital (combined)	\$112,000
Total	\$972,000

2014 Annual Report IPC accountability metrics

File management goals

- see diagrams below

Proactive compliance work

Work carried out by the Office of the Information and Privacy Commissioner (OIPC) to assist public bodies meet the ATIPP Act requirements

- provided comments to public bodies on seven policies or protocols, three information sharing agreements, two projects, and two privacy impact assessments
- identified 39 guidance needs
- issued Video Surveillance Guidance
- delivered four Privacy by Design workshops
- delivered five presentations (three general privacy awareness, one video surveillance, one privacy breach management)
- presented in three access and privacy conferences
- met with senior officials of all public bodies for annual review

- published one Inquiry Report, one Investigation Report, one case summary, and developed a sectional index including all published reports

Skills development

Participation by various OIPC staff or the IPC

- attended four conferences, two national meetings, four webinars, one presentation and four workshops

Complaints

No official complaints (in writing) were received in 2014

Two unofficial complaints:

- one about delays in completing a review which went to inquiry
- the second about confusion with a second memorandum of understanding to settle a mediation. Once the cause of the second complaint was identified, a process was developed to address the problem

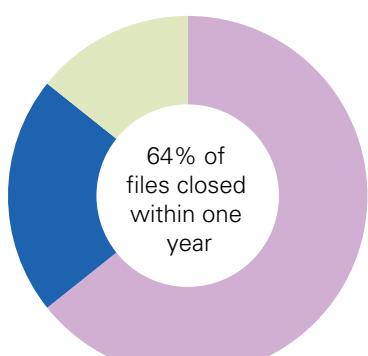
Public body	42 (b) Complaints	42(c) Comments	48 Reviews	Total	Recommendations	
					*Formal recommendations	Outstanding
Community Services			1 - 48(1)(a) 1 - 48(4)	2	1	0
Education	1	1 - privacy breach 1 - policy/protocol	1 - 48(1)(a) 1 - 48(1)(b) 1 - 48(1)(c) 1 - 48(3)	7		
Energy, Mines and Resources	1		2 - 48(1)(a) 2 - 48(1)(b)	5		
Environment	1		1 - 48(1)(a)	2		
Health and Social Services			1 - ISA 1 - PIA 1 - privacy breach	5		
Highways and Public Works	1	1 - legislation 2 - policy/protocol 2 - ISA	1 - 48(1)(b) 2 - 48(4)	9		
Justice	3	1 - legislation	2 - 48(1)(a) 2 - 48(1)(c) 1 - 48(1)(d) 1 - 48(2)	10		
Public Service Commission	4	2 - PIA	2 - 48(1)(a) 1 - 48(1)(c)	9	1	0
Yukon Housing, Liquor and Lotteries			1 - 48(1)(b)	1		
Yukon Workers' Compensation Health and Safety Board	1			1		
Yukon College		1 - policy/protocol		1		
Yukon Hospital Corporation		1 - PIA		1		
Records Manager (non-public body)		1 - policy/protocol		1	1	0
Other non-public body or multiple public bodies		1 - PIA 1 - privacy audit 1 - guidance		3		
Total	12	19	26	57	3	0

*Formal recommendations are those issued by the IPC in an Inquiry or Investigation Report in 2014.

ATIPP Act – 2014 activity

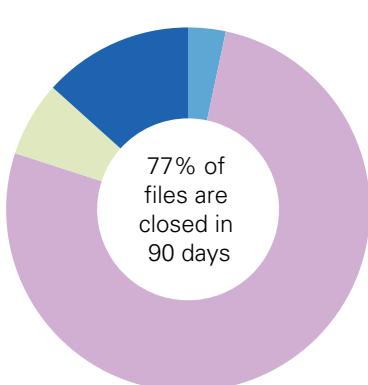
Resolved at intake – no file opened	
Non-jurisdiction	17
Referred-back	9
Requests for information	47
Informal complaint resolution	2
Total	75
Complaints and review files opened by type	
42 (b) administration complaint	12
48 (1)(a) refusal request for review	9
48 (1)(b) separation or obliteration request for review	5
48 (1)(b.1) abandoned request for review	0
48 (1)(c) time extension request for review	4
48 (1)(d) fee request for review	1
48 (2) correction/annotation request for review	1
48 (3) improper collection/use/disclosure of personal information request for review	2
48 (4) disclosure of third party business information request for review	4
Total	38
Comment files opened - 42 (c)	
Total ATIPP files opened in 2014	57
Total ATIPP files carried over from prior years	37
Total ATIPP files closed in 2014	30
Total files open as of December 2014 (includes carry over from prior years)	64

File management goals



Investigation files

- Closed within 1 year
- Still open (under 1 year)
- Still open (over 1 year)



Settlement files

- Closed within 90 days
- Closed after 90 days
- Still open (under 90 days)
- Still open (over 90 days)

1. What is a PIA?

A PIA (privacy impact assessment) is a tool which can be used by a public body to evaluate the risks of non-compliance with the ATIPP Act for any new or modified collection, use and disclosure of personal information.

Completing a PIA enables a public body, prior to collection, use or disclosure of personal information or any modification, to identify risks to privacy and develop a strategy to mitigate those risks. If the PIA is submitted to the OIPC, the PIA will be reviewed and comments and recommendations provided as needed to assist the public body meet its compliance obligations.

The ATIPP Act does not require a public body to submit a PIA to the OIPC. However, it is beneficial for a public body to have the OIPC review a PIA for several reasons. A public body is able to draw on the experience of the OIPC in interpreting and applying the ATIPP Act. It enables the public body to receive feedback from the OIPC about whether the project poses risks to the privacy of personal information. It demonstrates the public body's accountability for ensuring the

risks to privacy for projects involving personal information are being appropriately managed.

The OIPC recommends a public body complete a PIA for all new projects involving the collection, use and disclosure of personal information, such as in a new electronic information system, or where there is significant modification to an existing system, program or activity.

2. What is an ISA?

An ISA (information sharing agreement) is an agreement used when sharing personal information between a public body and another public body or private sector business. An ISA usually identifies the authorities for collection, use and disclosure of personal information and establishes the rules agreed to between the parties to protect the personal information. An ISA is commonly used for routine sharing of personal information or where large amounts of personal information will be shared. Like PIAs there is no requirement to submit ISAs to the OIPC for review. However, the benefits of doing so are the same as those identified for submitting PIAs.

3. What is an "opportunity to consult refused"?

Under the ATIPP Act, investigations are complaint driven. The IPC is not authorized to initiate an investigation without having first received a complaint. If the IPC becomes aware of a collection, use or disclosure of personal information by a public body that is or may be a violation of the ATIPP Act, the only recourse is for her to use her authority to provide comments to the public body on the implications for privacy protection. To obtain the information necessary to properly evaluate these implications and issue her comments, where a public body has not proactively sought the IPC's comments, the IPC can offer the public body an opportunity to consult with her. If a public body declines the offer or where it does not consult with her in a meaningful way that enables her to properly evaluate the implications to privacy, this is considered by the IPC to be an "opportunity to consult refused".