PUBLIC ENGAGEMENT ON THE COMPREHENSIVE REVIEW OF THE ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT

April 15, 2016

PUBLIC ENGAGEMENT - *ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT*

In 1996, the *Access to Information and Protection of Privacy Act* (the ATIPP Act, or the Act) came into force. The Act demonstrates the government's commitment to protecting privacy while still providing access to information. This legislation plays a critical role in maintaining government accountability and protecting the public's personal information.

Changes were made to the Act in 2004 and 2005 to respond to issues raised by stakeholders. Since then there have been a number of changes in Canadian policies, practices and legislation related to access to information or protection of privacy. A number of issues have also been raised by the Information and Privacy Commissioner (IPC), Members of the Legislative Assembly and other stakeholders. As a result, the Department of Justice committed to undertake a comprehensive review of the legislation. As part of that review the Department is seeking the public's views on changes to the Act.

The Department of Justice is interested in hearing your views on the specific issues and questions raised in this consultation paper, as well as any other comments or suggestions you may have regarding the reform of the *Access to Information and Protection of Privacy Act*.

This engagement paper contains:

Background - information on the Act including the work that has been done so far as part of the Comprehensive Review.

Issues and Questions - sets out the major components of the Act and the issues that have been raised, and poses questions for discussion.

The Public Engagement Feedback Form which is provided on the Department of Justice, GNWT Access and Privacy Office webpage can be used to provide comments. Please feel free to raise other issues that you think should be addressed.

The Department of Justice will be accepting responses to this paper until June 15, 2016. Responses can be sent by mail, fax or email to:

GNWT Access and Privacy Office, Department of Justice.
Mail: Box 1320, Yellowknife NWT X1A 2L9
Fax: (867) 873-0659
Email: ATIPP@gov.nt.ca

After the engagement process is completed, the Department of Justice will consider all submissions and prepare a proposal for changes to the legislation.

For a copy of the Act, Regulations or information related to the Act https://www.justice.gov.nt.ca/en/access-to-information-held-by-public-bodies/

BACKGROUND

The *Access to Information and Protection of Privacy Act* applies to public bodies that are set out in the regulations. This includes government departments, agencies, boards, commissions, corporations and offices. Individually these public bodies are responsible for responding to and making decisions about all access to information requests that they receive.

All public bodies have a designated access and privacy coordinator who is responsible for assisting the public with access to information requests as well as any questions they may have regarding privacy matters. Access and privacy coordinators undertake their responsibilities on a part time basis, and they do this work as part of other duties.

The Act also establishes the role of the NWT Information and Privacy Commissioner (IPC). The role of the IPC is to provide an independent review of the decisions made under the Act. The IPC may review the decision of a public body to not grant access to information, or correct personal information. The IPC may also review how a public body has collected, used or disclosed personal information.

The NWT *Access to Information and Protection of Privacy Act* does not apply to:

- Health Information –Access and privacy issues relating to individual health information are within the scope of the *Health Information Act*;
- Private Sector - Privacy protection in the private sector falls under the federal *Personal Information Protection and Electronic Documents Act;* and
- Government of Canada - Departments and Agencies – Access and privacy issues relating to federal departments or agencies, such as the RCMP, fall under the federal *Access to Information Act* and the *Privacy Act*.

Since the Act was introduced in the NWT in 1996 there have been a number of changes in Canadian policies, practices and legislation related to access to information or protection of privacy. Changes have been made to the Act in 2004 and again in 2005 to respond to issues that have been raised by stakeholders.

In 2012, the Department of Justice committed to commence a comprehensive review of the Act to address further issues identified by the GNWT as well as a variety of stakeholders including Members of the Legislative Assembly, and the Information and Privacy Commissioner.

Work on the comprehensive review includes:

1. Research and Jurisdictional Review

In the jurisdictional review provincial, territorial and federal legislation was considered for most issues, while a more in-depth examination and analysis was carried out on newer legislation or legislation that provided a range of approaches to the legislation. The GNWT Access and Privacy Office examined all sections of the Act taking into consideration the following:

1. Canadian policies, practices and legislation related to access to information and protection of privacy;
2. Provisions in the Act that may need clarifying so that the provisions can be interpreted and applied consistently;
3. Technological changes and advancements since the Act first came into force that may require changes;
4. Issues that have been raised by stakeholders.
5. Administrative functions of the Act (notices, time limits, extensions, fees) to determine if current requirements are still appropriate;

6. Proactive disclosure principles relating to access to information;
7. Exceptions to disclosure provisions of the Act that may need to be revised;
8. Privacy provisions of the Act to allow for integrated programs or initiatives and to determine if the current privacy provisions of the Act need to be enhanced to allow greater privacy protections; and
9. Review and appeal provisions, including the powers and duties of the Information and Privacy Commissioner, to determine if changes are needed to be made to improve the effectiveness of the current framework.

2. Consultation and Analysis

Stage Two of the comprehensive review involves conducting two major consultations:

1. Consultation with public bodies and the IPC - The first consultation was with GNWT Departments, Public Bodies (as set out in the ATIPP Regulations) and the Information and Privacy Commissioner on issues that have come out of the Stage One – Research and Jurisdictional Review. The consultation with Public Bodies and the IPC closed in January 2016.

2. Engagement with the public - The public engagement is the second major consultation, and is the purpose of this paper.

3. Development of Legislation

The third stage of the Comprehensive Review will be focused on the development of proposed legislation that reflects the information collected through the earlier stages - research and jurisdictional review, as well as consultations. The timing of this work will depend on the legislative priorities of the 18th Assembly.

ISSUES AND QUESTIONS

This section describes the related section of the Act, discusses the issues and poses questions for your consideration and response. The issues and questions are organized according to the following:

1. **PURPOSES OF THE ACT**
   - **1.1 Five Primary Purposes of the Act**

2. **THE SCOPE OF THE ACT**
   - **2.1 Records that do not fall under the ATIPP Act**
   - **2.2 Notwithstanding to ATIPP Act**

3. **ADMINISTRATION OF THE ACT**
   - **3.1 Access to Records**
   - **3.2 Time Limit for Responding**
   - **3.3 Extension of Time Limit for Responding**
   - **3.4 Fees**

4. **EXCEPTIONS TO DISCLOSURE**
   - **4.1 Application of Exceptions**
   - **4.2 Advice to Officials – Discretionary Exception**
   - **4.3 Disclosure Prejudicial to Law Enforcement– Mandatory/Discretionary Exception**
   - **4.4 Disclosure Harmful to an Applicant or Another Individual's Safety – Discretionary Exception**
   - **4.5 Confidential Evaluations– Discretionary Exception**
   - **4.6 Personal Privacy of Third Parties – Mandatory Exception**
   - **4.7 Business Interest of Third Parties – Mandatory Exception**

5. **RIGHTS OF THIRD PARTIES**
   - **5.1 Time Period for Third Party Consultation and Appeal**
   - **5.2 Time Period for Applicant and/or Third Party Appeals**

6. **REQUEST FOR REVIEW**
   - **6.1 Reviews on Privacy Complaints**

7. **PROTECTION OF PRIVACY**
   - **7.1 Collection of Personal Information**
   - **7.2 Collection of Information from Someone Other Than the Individual Concerned**
   - **7.3 Security of Personal Information**
     - **7.3.1 Privacy Impact Assessments (PIA)**
     - **7.3.2 Information Incident Reporting**
   - **7.4 Disclosures of Personal Information**

8. **THE INDEPENDENT REVIEW**
   - **8.1 Appointment**
   - **8.2 Recommendation Power**
   - **8.3 Powers of IPC on Review and Privacy Matters**

9. **OTHER MATTERS**
   - **9.1 Exercise of Rights by Other Persons**
   - **9.2 Offences and Penalties**
   - **9.3 Records Made Available Without Request**
   - **9.4 Review of the Act**

1. PURPOSES OF THE ACT

1.1 Five Primary Purposes of the Act

Access and privacy legislation was created to provide access to information that the government creates and receives, and to protect individual privacy rights related to that information.

The Act establishes the legal conditions for making public bodies more accountable to the public and protecting the personal privacy of our citizens.
These purposes are achieved by;

- providing the public with the right of access to information held by public bodies;
- providing individuals the right of access and the right to request corrections to their personal information held by public bodies;
- specifying the limited exceptions to the right of access;
- preventing the unauthorized collection, use or disclosure of personal information held by public bodies; and
- providing for an independent review of decisions made under the Act.

Issue

The purposes of the Act are intended to strengthen the rights of access to government records in the service of a more accountable and democratic government. It also enhances the protection of individual privacy rights in the personal information held by public bodies of the Government of the Northwest Territories (GNWT).

Some suggest the purposes of the Act do not go far enough in terms of making government information open and accessible.

Questions

a) *Do you think there are changes needed to the purposes of the Act, generally?*

b) *If yes, please explain why and what changes should be made.*

2. THE SCOPE OF THE ACT

2.1 Records that do not fall under the ATIPP Act

Under the ATIPP Act most records held by "public bodies" (GNWT Departments, boards, agencies) are subject to the Act. However there are a limited number of records that do not fall under the Act:

- records made from information in a NWT court file such as a record of a judge of the Court of Appeal, the Supreme Court or the Territorial Court or a justice of the peace;
- personal notes, communications or draft decisions of a person who is acting in a judicial or quasi-judicial capacity, such as the Rental Officer;
- records relating to an active prosecution;
- questions currently used on exams or tests or anticipated to be used in the future;
- materials placed in the NWT Archives by private sector companies or individuals;
- records made from information in a registry operated by a public body where public access is normally permitted.

If a public body receives a formal access to information request for these types of records, the applicant must be informed the Act does not apply to the requested information.

Issue

Access and privacy legislation across Canada provides a limited listing of records that are considered outside of the Act. These exceptions are very limited however this listing has not been assessed since the Act came into force.

Questions

a) *Is the current list of records that do not fall under the Act appropriate, or should some of these records be excluded? If so, please explain?*

b) *Are there other records that should also be excluded from the Act? If yes, what are they and why?*

2.2 Notwithstanding to ATIPP Act

The ATIPP Act defines the relationship between the Act and other NWT legislation. If a provision of the ATIPP Act conflicts with another piece of legislation, the ATIPP Act is considered to prevail unless the other legislation includes a "*notwithstanding to the Access to Information and Protection of Privacy Act*" clause. If such a clause exists the identified "provision" in this other piece of legislation applies even though it is not consistent with the ATIPP Act.

Legislation in the NWT that includes a notwithstanding to ATIPP clause is not common and is usually created to provide greater privacy protections, such as the new *Health Information Act* (HIA) or perhaps for enhanced disclosures provisions such as in the *Maintenance Orders Enforcement Act.*

Issue

Currently, there is no requirement to identify the different NWT Acts that are notwithstanding to ATIPP. This means that it may be difficult to get a good understanding of the exceptions to ATIPP that exist in NWT legislation. In some jurisdictions the Acts that include notwithstanding clauses are identified in the ATIPP regulations.

Question

a) *Should a listing of NWT Acts that include notwithstanding to ATIPP provisions be identified in the ATIPP Regulations?*

3. ADMINISTRATION OF THE ACT

The Act requires applicants who are making a formal access to information request to submit the request in writing to the public body they believe to have custody or control of the record. Applicants must also provide enough detail to enable the public body to identify the record. If the request is for general information, they must include the $25.00 application fee.

Currently, applicants can make a request using an official request for information form, available from the Department of Justice website, or by written letter requesting records and referencing the Act. Applicants who are unable to put forward a written request may submit an oral request.

3.1 Access to Records

Issue

When the Act came into force in December 1996, the procedures developed for processing access to information requests were based on a paper format. However, advances in technology have changed the way government does business and records created today are typically in an electronic format. While public bodies in the NWT currently provide documents to applicants in an electronic format, typically by a PDF version of the paper or electronic word version, there is no requirement to do so.

Question

a) *Should the Act require public bodies to provide an electronic or paper version of the requested information depending on the preference of the applicant?*

3.2 Time Limit for Responding

Public bodies are required to respond to a request for access to information within 30 calendar days after receiving it, unless the time limit is officially extended or the request is transferred to another public body. The time period begins on the date the request is received by the public body's access and privacy coordinator.

A public body that fails to respond to a request within the required 30 days is considered to have refused the applicant's request for records. This allows the applicant to immediately launch an appeal to the Information and Privacy Commissioner (IPC) regarding the refusal to provide records.

Issue

The current 30 calendar day timeframe is consistent with the majority of jurisdictions in Canada. As a smaller jurisdiction, NWT Access and Privacy Coordinators often fulfill their duties on a part time basis, and a shorter initial response time could prove difficult to implement. However, some critics have indicated that the government should consider shortening the initial response time.

Questions

a) *Do you think that the initial response time, which is currently 30 days, should be changed? Should it be shorter or longer?*

b) *If you think it should be changed, why?*

3.3 Extension of Time Limit for Responding

The Act allows public bodies to extend the time limit for responding to an applicant's request by a reasonable period, in the following circumstances:

- If the applicant did not provide enough detail to allow the public body to identify the requested records;
- If a large volume of records is requested or must be searched to identify the requested records which would require a longer response time;

- If more time is needed for the public body to consult with another public body or a "third party" (a person or business that may be affected by the request) and cannot respond to the request within the 30 day time limit; or
- a third party requests the Information and Privacy Commissioner to review the matter.

Public bodies that extend time limits are required to notify applicants that an extension is being taken, as well as the reason why there is an extension and the date when a response can be expected. Applicants must also be notified of their right to make a complaint about the extension to the Commissioner.

Issue

NWT public bodies make their own decision on what constitutes a "reasonable period" for a time extensions however this has resulted in an inconsistent approach.

Across Canada, the approaches to initiating a time extension are varied. The majority of jurisdictions have specific time frames of 15-30 days for extensions. In some instances, a public body may set an initial time period of 30 days but any longer requires the Information and Privacy Commissioner's permission.

Other jurisdictions require public bodies to apply directly to the IPC for approval of a time extension, in particular if they have received multiple concurrent requests from the same applicant(s).

Questions

a) *Do you think that a "reasonable period" for a time extension should be set out in the ATIPP Act?*

b) *If so, what is a reasonable time frame?*

c) *Should the public bodies have to make an application to the IPC for a time extension? If so why, if not why not?*

3.4 Fees

The ATIPP Act gives individuals the right to request access to general information held by public bodies as well as the right to request access to their own personal information.

The legislation allows fees to be charged to applicants requesting information and requires that applicants are provided with an estimate of those fees. Under the ATIPP regulations there are two separate types of fees; fees for applicants requesting access to their own personal information, (personal requests), and fees for applicants requesting access to general (non-personal) information. Public bodies must notify applicants that they have 20 days to accept the estimated fees or modify the request to change the amount of fees assessed.

General requests received by public bodies must include an initial $25.00 application fee. Other fees relating to the processing of a general request may apply. Following receipt of the initial application fee, public bodies must provide applicants with notice of the fees assessed in relation to their request. If the amount is lower than $150.00 the applicant will not be charged any fees however if the estimated fees exceeds $150.00, public bodies must charge the total amount and request 50% payment immediately.

Fees for personal information requests only include the cost of copying and shipping the record and only if the fees are in excess of $25.00.

The ATIPP Regulations also provides that public bodies, at the request of the applicant, may waive part or all fees if, in the opinion of the public body, the applicant cannot afford the payment or for any other reason it is fair to excuse payment.

Issue

The fees outlined in the legislation were never intended to cover the actual cost of administering formal access to information requests. Any fees charged are only intended to offset the costs of providing records to applicants and possibly to discourage frivolous requests. However, it is important that the fees charged do not become a barrier to access information.

The following table (Table 1) details the typical fees charged in relation to general and personal access to information requests, across Canada. Some jurisdictions have lowered or eliminated the initial application fees for general requests and photocopying fees have been decreased. Other jurisdictions have increased the hourly fees relating to locating and preparing records, which is somewhat offset by an increase in the number of "free" hours applicants may get.

Questions

a) *Are the current fees in the NWT, noted in the attached table, still appropriate? Do they create a barrier to access to information?*

b) *If you think they need to be changed, what do you suggest?*

3.4 Table 1. Fees for General and Personal Access to Information Requests

Fees for General Access to Information Requests				
Jurisdiction	**Application Fee**	**Hours Free**	**Location & Preparation of Records**	**Photocopy& Computer Printout**
NT	$25.00	N/A	$27.00 per hour if total cost exceeds $150.00	$0.25 per page if fees exceed $150.00
NU	$25.00	N/A	$27.00 per hour if total cost exceeds $150.00	$0.25 per page if fees exceed $150.00
YK	No fee	3 hours free	$25.00 per hour	$0.15 per page
BC	No fee	3 hours free	$30.00 per hour	$0.25 per page B/W $1.65 per page Colour
AB	$25.00	N/A	$27.00 per hour if total cost exceeds $150.00	$0.25 per page if fees exceed $150
SK	No fee	2 hours free	$30.00 per hour	$0.25 per page
MB	No fee	2 hours free	$30.00 per hour	$0.20 per page
ON	$5.00	N/A	$30.00 per hour	$0.20 per page
QB	No fee	N/A	No fee	No charge up to $7.45 then $0.38 page
NS	$5.00	2 hours free	$30.00 per hour	$0.20 per page
NB	No fee	N/A	No fee	No fee
PEI	$5.00	2 hours free	$20.00 per hour	$0.25 per page
NFLD	No fee	10 hours free	$25.00 per hour	$0.25 per page
Canada	$5.00	5 hours free	$10.00 per hour	$0.20 per page
Fees for Personal Access to Information Requests				
NT	No fee	N/A	No fee	$0.25 per page if fees exceed $25.00
NU	No fee	N/A	No fee	$0.25 per page if fees exceed $25.00
YK	No fee	3 hours free	$25.00 per hour	$0.15 per page (depends on paper size)
BC	No fee	N/A	No fee	No fee
AB	No fee	N/A	No fee	$0.25 per page / if fees exceed $10
SK	No fee	2 hours free	$30.00 per hour	$0.25 per page
MB	No fee	2 hours free	$30.00 per hour	$0.20 per page / if fees exceed $10
ON	$5.00 (?)	N/A	No fee	$0.20 per page
QB	No fee	N/A	No fee	No charge up to $7.45 then $0.38 per page
NS	No fee	N/A	No fee	No fee
NB	No fee	N/A	No fee	No fee
PEI	No fee	N/A	No fee	$0.25 per page
NFLD	No fee	N/A	No fee	No fee
Canada	$5.00	5 hours free	$10.00 per hour	$0.20 per page

4. EXCEPTIONS TO DISCLOSURE

4.1 Application of Exceptions

While the ATIPP Act provides the public with a right of access to records held by public bodies, public bodies may withhold records if they fall under one of the limited and specific "exceptions" set out in the Act.

The legislation provides for two types of exceptions, mandatory exceptions and discretionary exceptions. Records requested by an applicant, which are found to fall under a mandatory exception, must be denied. Currently there are five mandatory exceptions:

- section 13 cabinet confidences;
- section 20(3) a law enforcement record the disclosure of which is an offence under an act of Canada;
- section 23 disclosure harmful to personal privacy;
- section 24 disclosure harmful to business interests of a third party; and
- section 4 disclosure prohibited by another enactment of the NWT.

Records requested by an applicant which are found to fall under a discretionary exception must be reviewed to determine whether harm is likely to result from the release of information. If no harm is apparent the information should be disclosed. This is based on the belief that the public has a right of access to information held by public bodies unless there is harm in releasing it. There are ten discretionary exceptions:

- section 14 advice from officials;
- section 15 privileged information;
- section 16 disclosure harmful to intergovernmental relations;
- section 17 disclosure harmful to the economic or other interests of a public body;
- section 18 testing procedures;
- section 19 disclosure harmful to the conservation of heritage sites, etc.;
- sections 20(1)&(2) disclosure harmful to law enforcement;
- section 21 disclosure harmful to individual safety;
- section 22 confidential evaluations; and
- section 25 information that is or will be available to the public.

Applicants who are informed that records will be granted must be informed where, when, and how access will be given. If access to the records or portions of the records is refused, public bodies are required to provide applicants with clear explanations of their decisions, the provision(s) of the Act that apply and the reasons for the application of that provision(s) in this particular instance.

Issue

All access and privacy legislation across Canada provides for similar mandatory and discretionary exceptions to the right of access however the current listing of exceptions has not been reviewed since the Act came into force in 1996.

Questions

a) *Are the mandatory exceptions to disclosure appropriate? If not, please explain why and provide suggestions for improvement.*

b) *Are the discretionary exceptions to disclosure appropriate? If not, please explain why and provide suggestions for improvement.*

4.2 Advice to Officials – Discretionary Exception

The ATIPP Act provides a discretionary exception which is intended to protect discussions between senior officials and ministers, and their staff, as well as among officials themselves. Public bodies may refuse to disclose information if the disclosure could reasonably be expected to reveal:

- advice, proposals, recommendations, analyses or policy consultation questions developed by or for a public body or a member of Cabinet;
- consultations or deliberations involving officers or employees of a public body, members of Cabinet or their staff;
- positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations on behalf of the GNWT or a public body, or matters that relate to those negotiations;
- plans relating to the management of personnel or the administration of a public body that have yet to be implemented;
- the contents of draft legislation, regulations and orders;
- the contents of agendas or minutes of meetings of an agency, board, commission, corporation, or public body, or
- information including the proposed plans, policies or projects of a public body where the disclosure could result in the disclosure of a pending policy or budgetary decision.

This section of the Act clarifies the type of information that would not fall under this exception and that this exception does not apply to information older than 15 years.

Issue

All Canadian jurisdictions include a similar exemption within their legislation relating to "advice and recommendations" however the current list of information that falls within this discretionary exception has not been reviewed since the Act came into force.

Questions

a) Is the list of discretionary exceptions appropriate?

b) If not, please indicate what changes you would make and why.

4.3 Disclosure Prejudicial to Law Enforcement– Mandatory and Discretionary Exception

The Act allows public bodies to refuse access to records in order to protect both law enforcement activities and information in certain law enforcement records. The legislation defines law enforcement to include**:**

- policing, including criminal intelligence operations;
- investigations that lead or could lead to a penalty or sanction being imposed; and/or
- proceedings that lead or could lead to a penalty or sanction being imposed**.**

Public bodies may refuse to disclose information if the disclosure will likely:

- prejudice a law enforcement matter;
- prejudice the defence of Canada or of any foreign state or harm the detection, prevention or suppression of espionage, sabotage or terrorism;
- impair the effectiveness of investigative techniques and procedures used, or likely to be used;
- reveal the identity of a confidential source of law enforcement information;
- endanger the physical health or safety of a law enforcement officer or any other person;

- deprive a person of the right to a fair trial or impartial adjudication;
- reveal a record that has been lawfully confiscated from a person by a peace officer;
- facilitate the escape from custody of an individual who is being lawfully detained;
- facilitate the commission of an unlawful act or hamper the control of crime;
- reveal technical information relating to weapons or potential weapons;
- prejudice the security of any property or system, including a building, vehicle, computer system or a communications system; or
- reveal information in a correctional record, supplied explicitly or implicitly, in confidence.

Included in this section is a mandatory exception which requires public bodies to refuse access to a law enforcement record that contains information which if disclosed would be considered an offence under a federal Act. An example of this would be releasing the name of a young offender, as this is an offence under the federal *Youth Criminal Justice Act*.

Issue

Other jurisdictions include similar exceptions to disclosure in their access and privacy legislation, however many have expanded this section to include the following provisions:

Public bodies may refuse to disclose information if the disclosure will likely:

- *reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities;*
- *reveal information relating to or used in the exercise of prosecutorial discretion;*
- *adversely affect the detection, investigation, prevention or prosecution of an offence or the security of a center of lawful detention; and/or*
- *harm the conduct of existing or imminent legal proceedings.*

Questions

a) Should the NWT consider expanding the exemptions in this section, or making other changes?

b) If so what would you suggest, and why?

4.4 Disclosure Harmful to an Applicant or Another Individual's Safety – Discretionary

The Act allows public bodies to refuse to disclose information, including an individual's own personal information, if the disclosure could endanger another person's safety, mental or physical health.

Public bodies may consider refusing to disclose to an applicant information about him or herself if in the opinion of a medical or other expert, the disclosure could reasonably be expected to result in immediate and grave danger to the applicant's health or safety.

Issue

The majority of Canadian jurisdictions have expanded this provision to provide public bodies with discretion to refuse to disclose information that may interfere with "public safety". Public safety has been generally defined to mean information where the disclosure could hamper or block the functioning of organizations and structures that ensure the safety and well-being of the public.

Questions

a) Should the Act be broadened to address concerns about public safety?

b) If no, please explain why not?

4.5 Confidential Evaluations– Discretionary Exception

This exception allows public bodies to refuse to disclose to applicants materials that are part of an evaluation or an opinion, including the applicant's own personal information, if the information was compiled for the purposes of determining the applicant's suitability, eligibility or qualification for employment or for the awarding of government contracts.

Refusing this information is intended to protect the process where information is compiled about an individual, in order to assess or appraise his or her suitability.

Issue

The majority of Canadian jurisdictions include a section in their access and privacy legislation that allows a public body to refuse to disclose this type of information. The intent of this exception is to protect the receipt of confidential evaluations received by public bodies, particularly in relation to the hiring of personnel or awarding of contracts.

Questions

a) *Do you think that this type of discretionary exception should be maintained?*

b) *If no, please explain why?*

4.5 Personal Privacy of Third Parties – Mandatory Exception

Protecting the personal privacy of individuals is a key factor in relation to access to information requests. The Act provides that public bodies that receive a formal access to information request must not disclose personal information of "third parties", if the disclosure could be considered an unreasonable invasion of their privacy.

The Act also defines what is considered personal information. To qualify as personal information, information must be recorded, and it must be about an identifiable individual and not a group, organization or corporation. An individual is either named in the record or it is possible to identify the individual from the contents of the record.

The legislation provides examples of personal information which, if disclosed would be presumed to be an unreasonable invasion of a third party's personal privacy. Some examples include information that:

- relates to a medical, psychiatric or psychological history, diagnosis, treatment or evaluation;
- relates to employment, occupational or educational history;
- is obtained on a tax return or gathered for the purpose of collecting tax;
- describes the third party's finances, income, assets, liabilities, net worth, bank balances, financial history or activities or credit worthiness;
- consists of personal recommendations or evaluations, character references or personnel evaluations; or
- indicates the third party's race, religious beliefs, colour, gender, age, ancestry or place of origin.

When reviewing possible disclosures of personal information, the Act requires public bodies to consider a number of other factors, including but not limited to, whether the disclosure is desirable for the purpose of subjecting the activities of a public body to public scrutiny or if the disclosure would likely promote public health and safety or the protection of the environment.

However the Act also clearly indicates a number of circumstances when a disclosure of personal information is not considered an unreasonable invasion of personal privacy. For example if:

- the third party has, in writing, consented to or requested the disclosure;
- there is a compelling circumstance affecting someone's health or safety;
- the information relates to the third party's classification, salary range, discretionary benefits or employment responsibilities as an employee of a public body or employee of a member of the Executive Council; or
- the personal information relates to expenses incurred by the third party while travelling at the expense of the public body.

Public bodies that are considering disclosures under this section must consult with affected third parties through the formal ATIPP consultation process. Individual may consent to disclosure or provide a written response indicating the harms they perceive in relation to the information being disclosed. Public bodies must take the third party's concerns into consideration when deciding on possible disclosures.

Issue

All jurisdictions include in their legislation, exceptions relating to the protection of third party personal information. Some jurisdictions have expanded the examples of personal information, which if disclosed would be considered an unreasonable invasion of privacy, to include ethnic origin, sexual orientation and political beliefs or associations.

Examples of personal information which if disclosed are considered <u>not</u> to be an unreasonable invasion of third parties privacy includes the salary ranges of employees of public bodies. However some jurisdictions have indicated that the actual salary of employees and not just the salary range, should be disclosed in order to ensure transparency and accountability for public funds.

Another area of concern raised in relation to the personal information of third parties is how they apply to deceased individuals. Currently, the privacy protections of the Act apply whether an individual is alive or deceased however some jurisdictions have decided that the privacy interests of a deceased individual is considered to decrease over time and a disclosure after a set time period may not be considered an unreasonable invasion of privacy. Time limits reviewed range between 20-25 years before a disclosure may be considered.

Questions:

a) *Should the Act be changed to indicate disclosures of personal information relating to ethnic origin, sexual orientation or political beliefs would be considered an unreasonable invasion of privacy? Are there other examples that should be considered?*

b) *Should the examples of personal information, which if disclosed are <u>not</u> considered to be an unreasonable invasion of privacy, include the actual salary range of public servants? If not why?*

c) *Do the privacy interests of a deceased individual decrease over time? Or are there other factors that should be considered?*

4.6 Business Interest of Third Parties – Mandatory Exception

Public bodies that receive an access to information request relating to third party business information must consider if there is harm to the business if the information is disclosed. They must balance the public's expectation that they can access information relating to the business of government, against the protections the Act provides for third party business interests. All jurisdictions provide protections relating to third party businesses.

Under the Act there are seven distinct kinds of information that public bodies cannot disclose. They include, but are not limited to, information relating to trade secrets; financial, commercial, scientific, technical or labour relations information obtained in confidence from a third party; and information that could result in financial loss or prejudice the competitive position of a third party.

Public bodies that are considering disclosures under this section must consult with the business through the formal ATIPP consultation process. Businesses may consent to disclosure or provide a written response indicating the harms they perceive in relation to any disclosure. Public bodies must take the concerns raised into consideration when deciding on possible disclosures.

Issue

Currently this section does not include a provision that allows public bodies to refuse to disclose information that was supplied to, or the report of, an arbitrator, mediator, labour relations officer or body appointed to resolve a labour relations dispute. This type of provision is seen in other jurisdictions.

Questions:

a) *Should the Act be changed to include a section to protect information supplied to arbitrators, mediator, labour relations officers, or others relating to a labour dispute? If no, please explain why not.*

b) *Do you have any other concerns with the section that protects the business interests of third parties? If yes, what are they?*

5. RIGHT OF THIRD PARTIES

5.1 Time Period for Third Party Consultation

An applicant may request information held by a public body that includes third party information. A third party is considered someone other than an applicant or a public body. Third parties may be an individual whose personal information is contained in a record or it may include a private sector business whose interests may be affected by a possible disclosure of business information. The legislation is drafted to strike a balance between the interests of the third parties and the rights of an applicant.

Public bodies that are considering disclosing records that contain third party information are required to notify and consult with the third parties prior to any disclosure. The public body must provide the third party with a copy of the records and request their views on the disclosure. Third parties may consent to the disclosure or provide written responses explaining why the disclosure should not be made.

The public body must notify the applicant and third party of the public body's decision regarding access. The current legislated time frame for third party consultations is 120 days.

Issue

The 120 day time frames for third party consultation are, along with Nunavut, the longest time periods in Canada. Some applicants would like to see these time frames reduced.

Question

a) *Should the time frames for third party consultations and reviews be shortened? If yes, what do you consider reasonable time periods?*

5.2 Time Period for Applicant and/or Third Party Appeals

The legislation requires a public body to provide a written notice to the applicant and any affected third party of their decision on whether access will be provided to the requested documents. This notice of the decision does not include a copy of the requested document but rather details on what the documents are and if they will be disclosed. Applicants and third parties must also be provided notice that they have 30 days to request an appeal of the public body's decision to the Information and Privacy Commissioner.

Issue

While the current time frame of 30 days for appealing a decision of a public body to the IPC is in keeping with other jurisdictions, applicants and stakeholders have requested the time be extended due in part to the time it takes for mail services to northern communities.

Question

a) *Should the time frame relating to the 30 day appeal period for applicants and third parties be extended? If yes, what do you consider a reasonable time period?*

6. REQUESTS FOR REVIEW

Applicants or third parties who are not satisfied with a decision made by a public body have the right to an impartial review of that decision. This right of review is a fundamental principle of the Act and is intended to ensure that the Act is interpreted consistently and the purposes of the Act are achieved.

The legislation establishes the position of the Information and Privacy Commissioner (IPC) to review the decisions made by public bodies. Third parties who have been notified of a decision to give access to information in records that might affect their personal privacy or their business interests may also ask the IPC to review any decision the public body makes before any records are disclosed.

6.1 Reviews on Privacy Complaints

The Act provides applicants who have concerns relating to how a public body may have collected, used or disclosed their personal information to request a review of the matter to the IPC.

Issue

The NWT time frames of 90 days, relating to a privacy complaint process are, along with Nunavut, the longest time periods in Canada.

Questions

a) *Should the time frames relating to third party consultations and reviews related to privacy complaints be shortened?*

b) *If yes, what do you consider reasonable time periods?*

7. PROTECTION OF PERSONAL INFORMATION

7.1 Collection of Personal Information

The ATIPP Act restricts the collection of personal information by public bodies. Under the Act no personal information may be collected by a public body unless the collection of personal information:

- is specifically authorized by legislation (i.e. Maintenance Enforcement Orders Act.);
- is collected for the purposes of law enforcement, or
- relates directly to and is necessary for an existing or proposed program or activity of the public body.

Information is typically collected in an application form, interviews, questionnaires or surveys.

Issue

Unlike legislation in other jurisdictions, the ATIPP Act does not allow for the collection of personal information for the purpose of planning or evaluating a program or activity of a public body.

Questions

a) *Should the Act be changed to allow for the collection of personal information for program evaluation or planning?*

b) *If no, why not?*

7.2 Collection of Information from Someone Other Than the Individual Concerned

Public bodies are required to collect personal information directly from the individual the information is about. This is an important principle as it makes sure that individuals are aware of the personal information being collected about them.

Issue

The legislation lists the specific circumstances where a public body may collect personal information from sources other than the individual themselves, however it does not allow for the collection or disclosure of personal information for the delivery of common or integrated programs.

Programs that are shared between public bodies are required to create and administer a series of consent forms for the disclosure of information between public bodies, even though it's related to an integrated program intended to benefit the client. This can result in delays in the delivery of services to clients, and can require the client to fill out numerous forms with the same or similar information.

Other Canadian jurisdictions have addressed this issue by including a provision in their legislation that permits public bodies to collect personal information directly from other public bodies or agencies or disclose personal information to those agencies, if the information is necessary for delivery and evaluation of a common or integrated program or activity.

Questions

a) *Should the Act be changed to allow public bodies to collect personal information from someone other than the individual if it is for the purpose of providing information for integrated program services; or evaluating a common or integrated program or activity?*

b) *If no, please explain why not?*

7.3 Security of Personal Information

The ATIPP Act requires public bodies to protect personal information by making reasonable security arrangements against such risks as unauthorised access, collection, use, disclosure or disposal. This requires public bodies to take the necessary steps to implement privacy protections by implementing policies, practises and procedures relating to the protection of personal information in their custody and control. This relates to information collected directly by the public body or by a contractor on behalf of the public body.

In the GNWT there are a variety of privacy compliance policies, directives and tools that assist public bodies in this responsibility, including Privacy Impact Assessments (PIA), and Information Incident Reporting.

7.3.1 Privacy Impact Assessments (PIA)

A PIA is the principal tool used in Canada to ensure that programs and information technology systems and applications are compliant with the jurisdictions' privacy laws. The GNWT Access and Privacy Office has developed a PIA tool that assists public bodies in determining the overall level of privacy risk associated with a project involving personal information. Public bodies may also undertake a PIA for contracted services. The PIA process is designed to ensure that public bodies can evaluate the project or program for compliance with the privacy provisions of the Act.

Issue

While all jurisdictions in Canada use PIAs to some degree, the majority of jurisdictions provide for the use of PIAs in either government policy or directives, or in their access and privacy legislation.

Question

a) *Should PIAs be required in the NWT?*

b) *If yes, would the use of government policies and/or directives be acceptable or should it be defined in the legislation?*

7.3.2 Information Incident Reporting

In the GNWT, breaches of personal information are often referred to as an Information Incident. An Information Incident is an unwanted or unexpected event that threatens the privacy and/or security of our information. These events can be accidental or deliberate and include the theft, loss, alteration or destruction of information. Information incidents may include both security and privacy breaches.

Information incidents concerning a privacy breach may involve the unauthorized collection, use, disclosure, access, disposal, or storage of personal information, whether accidental or deliberate.

Issue

The requirements for privacy breach reporting vary across Canada. The majority of Canadian jurisdictions have policies or directives that set out what is required. Currently the GNWT Information Incident Reporting falls under a government directive.

Question

a) *Should information incident reporting continue to be addressed through the use of government policies and/or directives or should this be addressed in the legislation?*

7.4 Disclosures of Personal Information

The ATIPP Act identifies twenty two circumstances where public bodies may disclose personal information. Examples include, but are not limited to:

- if the disclosure is in keeping with why the information was originally collected or compiled
- if the individual the information is about consents to the disclosure
- if the information is for the purpose of collecting a fine or debt owing by an individual to a public body
- if the information is disclosed for law enforcement purposes:
- if the information is about employees and will be used for the purposes of hiring, managing or administering personnel of a public body.
- if the information is for the Maintenance Enforcement Administrator and involve personal information about individuals in default of their spousal maintenance payments; and
- if the information is provided to a Member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem.

In making decisions on disclosing personal information in these situations, public bodies must take into account any harm that could result from the disclosure and the consequences for the public body in withholding the information.

Issue

Disclosures may only occur in the specific circumstances outlined in the legislation. If the disclosure is not identified in the Act, public bodies cannot disclose the information.

A jurisdictional review of disclosures of personal information has identified provisions that are intended to permit disclosure in new areas. Examples of possible provisions include the following disclosures:

- *to an officer or employee of a public body, if the disclosure is necessary for the delivery of a common or integrated program or service (previously discussed in 8.2);*
- *to a representative of a bargaining agent, who has been authorized in writing by the employee the information is about, to make an inquiry;*
- *to the surviving spouse or relative of a deceased individual where, the disclosure is not an unreasonable invasion of the deceased's personal privacy;*
- *for the purpose of i)licensing or registration of motor vehicles or drives, or*
  ii) verification of motor vehicle insurance, motor vehicle registration or drivers licenses.
- *for the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside of Canada by government bodies of professions and occupations; and*
- *of information*
  - *i) disclosed on a social media site by the individual the information is about,*
  - *ii) was obtained by the public body for the purpose of engaging individuals in public discussion or promotion respecting proposed or existing initiatives, policies, or activities of the public body, and*
  - *iii) is disclosed for a use that is consistent with the purposes described above in (ii).*

Questions

a) *Should the Act be changed to permit public bodies to disclose personal information for the identified situations noted above? If yes, please identify the provisions that should be included and why?*

b) *Are there other situations requiring a disclosure of personal information from a public body, that should also be considered?*

8. THE INDEPENDENT REVIEW

8.1 Appointment

The ATIPP Act establishes the position of the Information and Privacy Commissioner (IPC). The IPC is an officer of the Legislature who is independent of government and provides an independent review of the decisions made under the Act. The IPC may review the decision of a public body to not grant access to information, or correct personal information and may also review how public bodies collect, use or disclose personal information.

Issue

Currently under the ATIPP Act an IPC may serve for five years or until they are reappointed or someone succeeds them. There is no limit on the number of terms that an IPC can serve.

Appointments for IPCs in Canada typically range between 5-7 years however the federal government and five other provinces and territories have restricted the IPC's term of office to either one term only (New Brunswick) or two successive terms, (Yukon, Newfoundland, New Brunswick, Manitoba and Saskatchewan).

Question

a) *Should the NWT IPC term of office be restricted? If yes, what should be the maximum length of term and how many terms should the IPC be allowed to serve?*

8.2 Recommendation Power

The NWT IPC has powers similar to an ombudsperson. The IPC has the authority to review decisions of the public bodies and may issues recommendations. The IPC's recommendations are not binding on the public body. If an applicant or third party does not agree with a decision of a public body, the applicant would need to appeal the decision on an access to information matter to the Supreme Court of the NWT.

In Canada, IPCs either follow the ombudsperson model (make recommendations), or the IPC is granted order making power. IPCs who have order making powers, (BC, Alberta, Quebec, Ontario and PEI) may issue decisions to public bodies that are legally binding.

Issue

Some stakeholders have suggested that in order to support greater accountability and transparency of public bodies the ATIPP Act needs to be amended to give the IPC order making powers.

There are pros and cons for both models. The current ombudsperson model supports the spirit and the intention of the Act in a collegial way. The ombudsperson model also provides the IPC flexibility in the recommendations as they are not a matter of law. However, if applicants need to appeal a decision to the Supreme Court, it was suggested that the costs and complexity they face may be a barrier.

The quasi-judicial order making-model would provide the Commissioner with the ability to issue legal orders, however the majority of jurisdictions have not supported this model as there are concerns it can become too formalized, resulting in a process that is nearly as expensive and time-consuming as court proceedings.

Questions

a) *Should the Act be revised to provide the NWT IPC with order making powers?*

b) *Are there other ways of addressing the issues raised?*

8.3 Powers of IPC on Review and Privacy Matters

In the NWT the IPC has specific powers in relation to a review. During a review of an access to information request, the IPC's has the ability to obtain and review all records required for an investigation, issue production orders, and administer oaths. The IPC may also enforce attendance of witnesses or compel any person to give evidence.

In relation to a privacy complaint the IPC has the authority to require public bodies to provide any document or allow her to examine any document pertaining to the request, and held by the public body.

Issue

Currently, the IPC's review powers do not allow for mediation between public bodies and applicants. In other jurisdictions such as Newfoundland, their legislation allows the IPC to attempt to resolve a request for review regarding access to information or a privacy complaint informally, to the satisfaction of the parties. If the matter is unable to be resolved informally, the IPC may then undertake a formal review of the matter.

Additionally, the current privacy complaint process only allows the IPC to undertake a review when a formal complaint has been received. If privacy issues come to the attention of the IPC either through the media or by individuals who are unwilling to file formal complaints, the ATIPP Act does not allow the IPC to initiate a privacy review into the matter.

Questions

a) *Should the Act be changed to allow the IPC to attempt to mediate access to information requests or privacy complaints?*

b) *Should the Act be changed to permit the IPC to initiate a privacy review even though a formal complaint has not been made?*

9 GENERAL AND OTHER MATTERS

9.1 Exercise of Rights by Other Persons

The ATIPP legislation sets out situations where other persons may be authorized to act on behalf of another individual in relation to specific functions of the Act. Someone may act on behalf of someone else if:

- an individual is deceased; their personal representative may act on their behalf in relation to the Act;
- a guardian or trustee has been appointed for the individual under *the Guardian and Trustee Act;*
- an individual is acting on behalf of a minor in their lawful custody; and
- an individual provides a written authorization that indicates they have written consent to act on behalf on another individual.

Issue

The majority of Canadian jurisdictions include provisions that allow someone to act on the behalf of another individual, and some have also included the following:

- *if someone is acting as an agent as designated under the Personal Directives Act.*
- *if someone is acting under the authority of a power of attorney. A power of attorney is an authority given to one person (called the attorney) to do certain acts in the name of, and personally representing, the person granting the power (called the donor).*

Question

a) *Should the Act be changed to include the exercise of rights by other persons as set out in a personal directive or a power of attorney? If no, please explain why.*

9.2 Offences and Penalties

The ATIPP Act indicates that a misuse of personal information is considered an offence. Any person who commits an offence is liable, upon conviction, to a fine of up to $5,000. It is an offence to:

- collect, use or disclose personal information in violation of privacy protections of the Act or the Regulations;
- obstruct the IPC or any other person in the performance of the duties, powers or functions of the IPC or any other person under the *Act*;
- fail to comply with any lawful requirement of the IPC or any other person under this *Act;* and
- make a false statement to, or mislead or attempt to mislead the IPC or any other person in the performance of the duties, powers or functions of the IPC or other person under the *Act.*

The Department of Justice is responsible for prosecuting offences under the Act and a court determines the amount of fine upon conviction.

Issue

Across Canada, fines in relation to offences under access and privacy legislation generally range from $1,000 to $10,000. Other jurisdictions have also included the following activities as offences:

- *if someone destroys records that are subject to the Act, or directs someone else to destroy records for the purpose of evading a request for access to the records, and,*

- *if someone either attempts to gain access or in fact gains access to personal information under which they have no authority to do so.*

Questions

a) *Should the fines associated with the offences be changed? If yes, what amount?*

b) *Should the offence portions of the Act be changed to include either of the two activities noted above? If no, why not?*

9.3 Records Made Available Without Request

Currently, the legislation allows public bodies to specify categories of records that are in their custody or under their control that will be made available to the public without a request for access under the Act. In addition, a public body may set reasonable fees for the provision of this information.

Issue

This section permits public bodies to specify categories of record that are available without an access to information request, however it does not require this to be done. In British Columbia, it is a requirement under their legislation for public bodies to establish categories of information that is available to the public without a formal request.

Question

a) *Should the Act be changed to require public bodies to establish categories of information that the public can access?*

9.4 Review of the Act

Issue:

The ATIPP Act does not include provisions that require the government to undertake a comprehensive review of the Act, on a regular basis. The majority of jurisdictions require a review be undertaken, generally every 5- 7 years.

Question

a) *Should the Act be revised to include the requirement for a regular comprehensive review of the legislation? If so, how often should this review happen?*