BECOMING A LEADER IN ACCESS AND PRIVACY

Submission to the 2013
Government of Alberta
FOIP Act Review

Office of the Information and
Privacy Commissioner of Alberta

On June 13, 2013, the Government of Alberta (GoA) announced the start of its review of the *Freedom of Information and Protection of Privacy Act* (the FOIP Act). As part of this review, the Honourable Donald Scott, Associate Minister of Accountability, Transparency and Transformation issued a *Discussion Guide*, launched a consultation process, and invited submissions from stakeholders and interested parties.

In response to the Associate Minister's invitation, I am pleased to submit this report, *Becoming a Leader in Access and Privacy*, which contains ideas, suggestions and recommendations for amending the FOIP Act such that Alberta's access to information and protection of privacy legislation might become a leading example for other jurisdictions. I have also prepared a separate submission which contains recommendations for technical amendments to the FOIP Act.

My Office has more than 17 years of experience overseeing compliance with the FOIP Act and has interpreted, mediated, investigated and issued orders, reports and decisions on hundreds of matters. As such, I believe that we have a unique understanding of the legislation, its relationship with other laws and its application to a diverse range of public bodies with their respective challenges and environments. Any changes, even seemingly minor ones, may result in unintended consequences. Given this, I ask that my Office be consulted throughout the FOIP Act Review and afforded the opportunity to comment on any proposed amendments to the FOIP Act.

I hope that *Becoming a Leader in Access and Privacy* will generate further thought and dialogue to inform the GoA's review of the FOIP Act.

Jill Clayton
Information and Privacy Commissioner
Office of the Information and Privacy Commissioner of Alberta
July 2013

CONTENTS

INTRODUCTION

The significance of access to information and privacy rights cannot be overstated. As former Supreme Court of Canada Justice Gérard V. La Forest stated in his 2005 report on the federal Offices of the Information and Privacy Commissioners, the rights protected by access to information and privacy legislation "are of the highest importance in the functioning of a modern democratic state." [1]

The right to access information held by public bodies promotes government accountability and transparency and enables the public to more fully and effectively participate in the democratic process as it is information that allows citizens to scrutinize government decisions and actions.

The right to control your own personal information, to decide to whom and when you shall reveal such information, is fundamental to individual dignity and integrity. There may be situations where a person may be compelled to reveal personal information but, when this is the case, there is also an expectation that the information will remain confidential and its use restricted to the purposes for which it was divulged. [2]

That the Legislative Assembly of Alberta considered these rights to be important is evidenced by its passage of the FOIP Act in 1994 (in force October 1, 1995). These rights are expressly stated in section 2 of the Act.

It is against this background that any discussion of changes to the FOIP Act must be considered. Any changes to the legislation should strengthen, not diminish, access to information and privacy rights.

Access to information and protection of privacy matters to Albertans

On June 13, 2013, I released the results of a public opinion survey commissioned by my Office. The telephone survey of 800 residents across Alberta was conducted between March 22-27, 2013. The survey results showed that:

- 97% of respondents believe it is important to protect the privacy of personal information; however, only 39% feel secure about the privacy of their own personal information.
- 93% of respondents believe it is important to protect the right to access information; but only 38% were confident about their own ability to access information.

[1] La Forest, Gérard V., *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*, Report of the Special Advisor to the Minister of Justice (Canada), November 15, 2005 (http://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/ip/toc-tdm.html)

[2] see *R. v. Dyment*, [1988] 2 S.C.R. 417 at 429-30; *Dagg v. Canada (Minister of Finance),* [1997] 2 S.C.R. 403 at 434-435; *R v. Duarte*, [1990] 1 S.C.R. 30 at 46

Strong legislation is not enough…

On April 9, 2012, the Centre for Law and Democracy (CLD) released the results of a comparative study that looked at access to information legislation from Alberta, British Columbia, Ontario and Nova Scotia. In the report, Alberta's legislation was ranked the lowest of the group.[3]

The CLD study provided helpful insight into possible improvements to strengthen access to information legislation. However, the CLD study was limited to assessing legal frameworks and did not measure quality of implementation. In releasing the results of its study, the CLD said:

> *In some cases, countries with relatively weak laws may nonetheless be very open, due to positive implementation efforts, while even relatively strong laws cannot ensure openness if they are not implemented properly. Regardless of these outlying cases, over time a strong access to information law can contribute to advancing openness and help those using it to defend and promote the right of access to information.*

I agree that strong access to information legislation can contribute to openness and promote access rights – however, the quality of implementation is equally as important.

In *Getting Accountability Right with a Privacy Management Program*,[4] produced by the Offices of the Information and Privacy Commissioner of Alberta and for British Columbia (AB OIPC and BC OIPC) in conjunction with the Office of the Privacy Commissioner of Canada (OPC), the Commissioners identified organizational commitment and senior leader support as primary building blocks of a culture of privacy. The same is required to build a culture of access. In addition, adequate resources (staffing, training) are required to ensure quality implementation.

I encourage the GoA and heads of all public bodies to lead by example and adopt a culture that respects and balances both access and privacy, and to ensure adequate resources are allocated to administering the FOIP Act and fulfilling legislative obligations.

" … even relatively strong laws cannot ensure openness if they are not implemented properly."

[3] http://www.law-democracy.org/live/legal-work/legal-analyses

[4] http://www.oipc.ab.ca/Content_Files/Files/Publications/Accountability_Doc_April_2012.pdf

RESPONSE TO DISCUSSION GUIDE

In June 2013, the GoA released a *Discussion Guide* as part of its consultation initiative for the FOIP Act Review.[5] The *Discussion Guide* solicited stakeholder views on four specific themes:

1. Making the FOIP Act clear and user-friendly
2. Open Government and the FOIP Act
3. Sharing personal information to provide programs and services; and
4. Addressing technological innovation.

My comments, ideas, suggestions and recommendations on each of these four themes are set out below.

1. Making the FOIP Act clear and user-friendly

The FOIP Act will be 18 years old on October 1, 2013. The legislation has been reviewed three times by all-party committees; the 1998-1999, and 2001-2002 reviews resulted in amendments to the legislation.[6]

Albertans are fortunate that the FOIP Act has been reviewed, updated and modernized over the years. However, it has been a number of years since the Act was last amended. In my view, the current FOIP Act Review provides an opportunity to revisit some of the basic principles of the legislation with an eye to making it work better for the public and stakeholders.

Scope of the Act

The FOIP Act grants a right of access to *any* record in the custody or under the control of a public body subject to specific and limited exceptions. The range of provincial publicly-funded entities is broad; however, not all are subject to the FOIP Act.

In addition, section 4(1) of the FOIP Act excludes certain types of records from the scope of the legislation. If a record falls within one of the exclusions of section 4(1), for example, the FOIP Act does not apply and the public has no ability to make a formal access request for the record, nor does the public body have any obligation to disclose the record.

The right of access under the FOIP Act also does not extend to certain records described in section 6(4) (records created solely for the purpose of briefing a member of the Executive Council assuming responsibility for a ministry or in preparation for a sitting of the Legislative Assembly) and section 6(7) (records relating to an audit by the Chief Internal Auditor of Alberta).

Given the increasingly-heard commitments to "accountability", "transparency" and "openness" – not only within Alberta but also across Canada and globally – any review of the FOIP Act should consider the scope of the legislation and whether it should extend to additional provincial publicly-funded entities. Further, existing exclusions under the Act should be reviewed and confirmed to be necessary.

[5] http://alberta.ca/AlbertaCode/images/FOIP-Act-Review-2013-Discussion-Guide.pdf

[6] Recommendations from the 2010 review of the FOIP Act were not implemented

Recommendation:

- Review the scope of the FOIP Act to ensure that publicly-funded entities that should be captured are. Confirm the ongoing need for exclusions.

Exceptions to access

Under the FOIP Act, a public body must disclose records/information responsive to a formal access request unless the public body is authorized to withhold that information under an exception to access as set out in the Act. Some of the exceptions to access are mandatory and some are discretionary. If a mandatory exception applies, a public body has no choice; it must refuse to provide access. However, if information falls under a discretionary exception, a public body may still decide to disclose the information.

Some of the exceptions in the FOIP Act are limited in that they no longer apply after a certain time period has elapsed. For example: sections 21(4), 22(2)(a), 23(2)(b), 24(2)(a) and 24(2.2) require that 15 years or more must pass before the exception no longer applies.

Recommendation:

- Review the exceptions to access set out in the FOIP Act to ensure they are as narrow and limited as possible.

Understanding and promoting the legislation

The GoA *Discussion Guide* states that "[t]he GoA recognizes the need for citizens to understand their access and privacy rights" and notes that "there are many questions about access and privacy."

Most of the questions included in this section of the *Discussion Guide* appear to be directed towards users of the legislation – that is, parties that use the FOIP Act to obtain access to personal or general information held by public bodies, or who may have concerns about the privacy of their own personal information.

As previously noted, the FOIP Act has been reviewed, updated and modernized over the years. However, it may be the case that the cumulative effect of 17 years of interpreting the Act, multiple reviews, and the increasing complexity of issues arising under the legislation, have contributed to a lack of clarity.

In my opinion, many of the challenges facing the FOIP Act stem from the need for greater clarity in its language and understanding of its principles. In some jurisdictions, this is accomplished directly through legislative provisions that, among other things, require the appointment of dedicated officials to assist in

OIPC 2013 Public Opinion Survey

- 69% of respondents were aware of laws to protect their personal/health information.
- 48% were aware of laws to provide individuals with the right to access information.
- 79% were aware they could request access to their own personal/health information.
- 69% were aware they had a right to request access to general information held by public bodies.

the implementation of the law, provide assistance to applicants, promote training, undertake reporting, and produce information about the law and the public's access to information rights.[7]

Recommendations:

- Review the wording of the FOIP Act with an eye to making it more "plain-language" and understandable for the public and stakeholders.
- Ensure adequate resources are allocated to providing educational resource materials for both the public and stakeholders (e.g. Frequently Asked Questions and Bulletins produced by Service Alberta). Develop and provide cost-effective FOIP training options.

Fees

Under section 93(1) of the FOIP Act, a public body may require an applicant to pay fees for services related to processing a formal access request. The fees are set out in sections 10-14 and Schedule 2 of the FOIP Regulation. Fees charged may include: an application fee; some costs for searching, locating and retrieving records; producing a record from an electronic record; and costs for shipping, etc. Applicants are entitled to receive a fee estimate before their request is processed, and may request a fee waiver in certain circumstances. An applicant may ask my Office to review fees charged to process a request for access and a decision to refuse a fee waiver request.

Anecdotally, my Office has heard that the fee schedule is cumbersome to administer and that the fees do not come close to covering the real cost of responding to access requests.

In my view, while it is reasonable to charge a nominal fee to provide access – this helps to prevent frivolous requests – it is important that fees not be a deterrent to access.

Recommendations:

- Review the current fee requirements to ensure that fees are appropriate and not a barrier to access.
- Review current fee provisions and schedule to ensure they are clear and understandable.

Separating the Act

While not specifically mentioned in the GoA FOIP Act Review *Discussion Guide*, the consultation sessions held by the Associate Minister and Service Alberta in June 2013 asked participants for their thoughts about separating Part 1 of the FOIP Act (access to information) from Part 2 (protection of privacy). It was suggested that this might help to make the FOIP Act clearer and more user-friendly; however, in the absence of any proposals for a legislative framework to replace the current one, it is not clear to me at this time how separating the FOIP Act would accomplish this objective.

While there are, no doubt, pros and cons associated with either approach, I would suggest the issue merits further study.

Recommendation:

- Before making any decision or recommendation to separate the two parts of the Act, it is important to clearly identify the objective that is to be achieved and how separating the Act would achieve it. A thorough cost-benefit analysis should also be undertaken.

[7] http://portal.unesco.org/ci/en/file_download.php/fa422efc11c9f9b15f9374a5eac31c7efreedom_info_laws.pdf

2. Open Government and the FOIP Act

In a March 2010 Working Paper commissioned by the Access to Information Program at the World Bank Institute and titled "Proactive Transparency: The future of the right to information?," author Helen Darbishire states:

> *There are two main ways by which information held by public bodies can be accessed by the public. The first is when individual members of the public file requests for and receive information (reactive disclosure). The second is when information is made public at the initiative of the public body, without a request being filed. This is known as proactive disclosure and the result is proactive transparency which can be achieved using a multiplicity of means….* [8]

The current FOIP Act Review offers an opportunity to consider how legislative amendments might be used to facilitate proactive transparency.

Proactive disclosure

As stated above, there is a "multiplicity of means" that may be used to achieve proactive transparency. One such means is a legislated duty to identify records that will be proactively disclosed without the need for a formal access request.

Darbishire's Working Paper cites access to information legislation in jurisdictions such as Mexico and India as examples in which specific classes of information are identified for proactive disclosure without the need for access to information requests. Mexico, Slovenia and the United States are also noted as jurisdictions in which public bodies are required to proactively disclose frequently requested records.

The United Kingdom's *Freedom of Information Act* requires public authorities to implement publication schemes, approved by the Information Commissioner's Office (ICO), and to publish information covered by the scheme. The ICO created a model publication scheme which requires public authorities to:

- commit to publishing certain classes of information;
- specify how the information will be made available and what fees will be charged for the information; and
- outline how the public authority will inform the public about the scheme.[9]

Currently, under section 88(1) of Alberta's FOIP Act, a public body has the discretion to specify categories of records that will be publicly available without a formal access request; however, this is not a mandatory requirement. Even if a public body should identify records, there is no requirement to make the information proactively available.

A legislated obligation under the FOIP Act for public bodies to proactively disclose information would have more force than a voluntary or policy requirement as it could be enforced through the review/order-making powers of my Office. It may also result in the added benefit of reducing the number of formal access requests received by public bodies through routinizing the disclosure of frequently requested records.

[8] http://siteresources.worldbank.org/EXTGOVACC/Resources/DarbishireProactiveTransparency.pdf

[9] www.ico.org.uk

Recommendations:

- Amend the FOIP Act to require public bodies to identify categories of records that will be made publicly available without requiring formal access requests. Require public bodies to make these records available.

- Establish minimum standards for proactive disclosure to provide guidance to public bodies and consistency to the public. Minimum standards could include:

    - specifying in legislation certain categories of records that public bodies must make available, such as: expenses, contracts over a certain dollar value, audit reports, etc.

    - requiring public bodies to establish publication schemes that identify classes of records that will be made available, methods by which the information will be made accessible, fees (if any) that may be charged, and how the public body will make the publication scheme available to the public. Consider requiring public bodies to submit publication schemes to my Office (or alternatively, a government ministry) for review and comment.

Disclosure logs

A disclosure log is a term used to refer to the proactive disclosure of information that has been released in response to an access request, and that is likely to be the subject of another request. In British Columbia, for example, the government posts copies of responses to many, but not all, general access requests on its Open Information website. In some jurisdictions (e.g. the United States, Mexico) access to information laws require the information be made available electronically.

Recommendation:

- Consider amending the FOIP Act to include a duty for public bodies to publish responses to general access requests. Minimum standards should be developed to ensure consistency and that information that could potentially be harmful is not released.

Access Impact Assessments

Many public bodies are familiar with the concept of a Privacy Impact Assessment (PIA) – a comprehensive review of a particular initiative, scheme or program that identifies, among other things, legislative authorities, information flows, potential privacy risks and mitigation strategies.

An Access Impact Assessment (AIA) is similar to a PIA but with a focus on access to information as opposed to privacy. An AIA examines how public bodies can fulfill their access to information obligations in relation to a proposed initiative, scheme or program.

By building in the principles of access to information at the design stage, a culture of openness and transparency is fostered and can further assist in identifying opportunities for proactive disclosures.

Recommendation:

- Require public bodies to complete and submit AIAs to my Office on proposed initiatives, schemes or programs that meet certain criteria (e.g. information sharing initiatives, data matching initiatives).

Records and information management

> *Good information management is a prerequisite of good decision-making, good program and service delivery and of accountability.*[10]

Good information management is also fundamental to achieving the goals of access and privacy legislation. Among other things, it helps to ensure that responses to access requests are complete, accurate and timely, and that records are properly secured and disposed of when appropriate.

There appears to be a trend across the country, however, that suggests information and records management activities, duties and responsibilities may not be receiving the respect and attention they are due.

In Alberta, the *Records Management Regulation* (RMR) sets out the authorities and requirements for records management in the GoA.[11] Each government ministry is responsible for setting its own records retention and disposition schedules. Despite this, in a report issued in November 2011 examining the Alberta Government's management of ministerial emails, former Commissioner Frank Work noted his concern that some ministry records were not covered by any records retention and disposition schedule. He recognized that "[t]his becomes an issue if those records are the subject of an access request or a complaint of improper destruction under the FOIP Act."[12]

More recently, in March 2013, the Information and Privacy Commissioner for BC released an investigation report concerning the number of "no responsive records" replies by the Government of BC to access requests.[13] The report recommended that the BC access to information legislation be amended to include a legislated duty to record key decisions. Similar recommendations calling for a "duty to record" were made in a special investigation report issued in June 2013 by the Information and Privacy Commissioner of Ontario.[14]

I am not aware of any specific provisions in Alberta's RMR or any policies that require that records be created in specific circumstances.

Under section 53(1)(a), I may conduct investigations to ensure that public bodies comply with rules relating to the destruction of records, which may be set out in enactment such as the RMR or in a bylaw, resolution or other legal instrument. However, there are no provisions under the FOIP Act requiring that public bodies document key decisions.

Recommendation:

- Ensure appropriate statutory and policy framework for records and information management is in place to support transparency, accountability and compliance with the FOIP Act. This could include an amendment to require that public bodies:

  - create such records as are reasonably necessary to document their decisions, actions, advice, recommendations and deliberations.

  - ensure that all records are covered in records retention and disposition schedules.

[10] http://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/atia-lai/index.html

[11] The RMR does not extend to other public bodies such as schools, municipalities, etc. Consequently, records and information management practices in Alberta are varied.

[12] http://www.oipc.ab.ca/Content_Files/Files/Orders/Report-Ministerial-Email-Investigation.pdf

[13] http://www.oipc.bc.ca/report/investigation-reports.aspx

[14] http://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=9181

3. Sharing personal information to provide programs and services

The OIPC's 2013-2016 Strategic Business Plan identifies a number of trends and issues having potentially significant access and privacy implications. One of these is the current predilection towards multi-agency citizen-centred service delivery, described as follows:

> *This global trend seeks to replace the traditional delivery of public service by myriad, disparate government agencies with a network of public, private and non-profit groups that come together to achieve a common mission or program outcome…The foundation that underpins multi-agency citizen-centred delivery of government services is the sharing of information beyond the sectoral boundaries of private, public, and health, and, in some cases, across provincial and national borders…*

This kind of information sharing can have significant implications for access and privacy including:

- Information sharing initiatives that remove consent requirements reduce individuals' ability to say yes or no to the sharing of their own personal information which is, fundamentally, what privacy laws are intended to provide – control.

- Removing consent requirements and allowing for indirect collection of personal information can undermine fundamental privacy principles of transparency, openness and accountability, and reduce individuals' ability to exercise their rights to complain or ask for a review under existing privacy laws.

- A basic principle of privacy requires that only the minimum amount of personal information required for specific purposes should be collected, used or disclosed. Information should only be used or disclosed for other purposes with consent or if authorized by legislation. Information sharing for broad purposes dilutes this privacy principle.

- Information sharing for broad purposes can increase the amount of personal information collected, used or disclosed by public bodies and increases the potential risks for unauthorized access, collection, use and disclosure. In addition, in the event of a breach, there is a greater potential risk of harm to affected individuals given the increased amount of personal information.

- Information sharing initiatives may involve parties that are not regulated by privacy legislation and not subject to any independent privacy oversight body.

- Information sharing initiatives that do not take into consideration current legislative language (in the *Health Information Act* (HIA), the *Personal Information Protection Act* (PIPA) and the FOIP Act) can introduce new tests, inconsistencies, and confusion, ultimately undermining existing privacy laws and increasing stakeholders' reluctance to share information.

Despite the above, I am not, in principle, opposed to information sharing initiatives. On the contrary, in many cases information sharing is beneficial, if not vital, to providing programs and services.

Alberta's three access and privacy laws – the FOIP Act, HIA and PIPA – also recognize that information can and should be shared in some circumstances. Each law sets out the circumstances in which personal and health information may be disclosed, either with or without consent. Section 40(1) of the FOIP Act,

for example, lists 37 circumstances in which personal information may be disclosed. In addition, other laws occasionally override the FOIP Act (referred to as "paramountcies") or otherwise authorize information sharing.

Despite these provisions in the FOIP Act and other laws, my Office frequently hears that information is not shared because workers do not understand or are fearful of contravening privacy laws. While I understand this may be a problem, the appropriate solution likely involves education and training, as opposed to legislative amendments.

Training and Education

- 44% of respondents have an access training and education program in place;
- 51% have a privacy training and education program.

OIPC 2012 Stakeholder Survey

Overall, while I acknowledge and respect the need to share information in order to provide programs and services, and to realize economic efficiencies and other benefits, this should not come at the expense of privacy. I maintain that, for any information sharing initiative, privacy implications must be thoroughly considered and proper controls in place to minimize potential risks. Information sharing should not override privacy rights except in specific and limited circumstances that are transparent to the public.

Recommendations:

- Proposed information sharing initiatives must be thoroughly reviewed and assessed for access and privacy implications before implementation to determine whether or not they are required. This includes ensuring that any legislative amendments are harmonized among the FOIP Act, HIA and PIPA to avoid introducing inconsistencies.
- Dedicate resources to education, training and resource materials.
- Include a requirement in the FOIP Act that all cross-sectoral information sharing initiatives be registered with my Office or a designated government ministry. The registry listing could document the nature of the information sharing initiative, names of participating stakeholders, and contact information of an officer/employee who can answer questions about the collection, use, disclosure, retention, security or destruction of personal/health information. The registry should be regularly updated and easily accessible to the public.
- Legislative schemes authorizing information sharing without consent must ensure that all participants are subject to Alberta's information and privacy laws.
- Include a requirement in the FOIP Act that public bodies must conduct and submit privacy impact assessments to my Office for information sharing initiatives that involve data matching and for any cross-sectoral initiatives.

- Stakeholders participating in cross-sectoral information sharing initiatives should be required to record disclosures, including disclosures via information systems, comparable to section 41 and section 41(1.1) of the HIA:

    - the name of the person/service provider to whom the information was disclosed;
    - the date and purpose of the disclosure; and
    - a description of the information disclosed.

- Legislation should ensure that individuals who are the subject of the information sharing have an express right to ask for access to and a copy of the disclosure notes. Individuals should also have a right to ask me for a review in relation to their requests (similar to section 41(3) of HIA).

4. Addressing technological innovation

As already noted above, the OIPC's 2013-2016 Strategic Business Plan identifies a number of trends and issues having potentially significant access and privacy implications. Many of the most significant of these are related to ubiquitous technology. This is evident in, for example:

- the increased use of social media by individuals and businesses to communicate, share and disseminate information online;

- the increasing prevalence of mobile devices (smart phones, laptops, iPads, and USB keys) which means that information is always on the go, never stationary, and not confined to any one jurisdiction;

- the enhanced ability of businesses and government to collect enormous amounts of information about citizens and to analyze the data in ways never previously contemplated.

Ubiquitous technology can be challenging because it is constantly changing, becoming outdated and replaced with new technological innovations at an ever increasingly rapid rate. The FOIP Act Review must consider and respond to ubiquitous technology, but it is also critical that the legislation be technologically-neutral or risk becoming quickly outdated and inapplicable.

I believe requirements such as access impact assessments, privacy impact assessments, and mandatory breach notification are solid measures that will support and protect the access and privacy rights of Albertans regardless of changes or advancements in technology.

Access and Privacy Impact Assessments

Under the HIA, health custodians are required to submit a PIA to my Office for review and comment before implementing new systems that affect health information. My Office sees benefits from the mandatory PIA requirement under HIA: we have a current and updated provincial perspective of initiatives involving health information, and PIAs are helpful in assisting custodians to comply with their obligations under HIA.

There is no corresponding requirement under the FOIP Act for public bodies to submit PIAs to my Office, although some public bodies choose to do so.

In his submission to the Standing Committee of Health for the 2010 FOIP Review, Commissioner Work said:

> *I believe there should be a mandatory requirement for public bodies to prepare privacy impact assessments in certain circumstances. The intent of this requirement is not to impose a burden on public bodies but to assure Albertans that the public bodies have fulfilled their due diligence and their statutory obligation under the FOIP Act in ensuring that Albertans' privacy is protected. The circumstances could be outlined in the FOIP Regulation and could include the following:*
>
> - *Initiatives involving multiple public and/or non-government bodies that result in the collection, use and disclosure of personal information.*
>
> - *When public bodies use a service provider outside Canada to collect, use, disclose or store personal information.*

I fully support this recommendation. A PIA is a useful tool for identifying potential privacy risks and how these risks could be mitigated. In addition, as already noted above, I support the concept of mandatory AIAs for certain initiatives.

Recommendation:

- Require public bodies to complete and submit privacy and access impact assessments to my Office on proposed initiatives, schemes or programs that meet certain criteria (for example, information sharing initiatives as discussed above).

Mandatory breach reporting

Under Alberta's private sector privacy law (PIPA), organizations must report a breach of personal information to my Office where they determine there is a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure of personal information. I have the power to require an organization to notify affected individuals.

Like private sector businesses, governments have the ability to collect an enormous amount of personal information about individuals and to analyze that information through technology in ways never previously contemplated. In the event of a breach, there is a greater risk of harm to individuals affected given the greater amount of personal information.

Additionally, the sharing of personal information across sectoral boundaries and in some cases, across provincial and national borders increases the risk of potential privacy breaches.

Notification allows an individual whose personal information has been compromised to take measures to protect themselves against such risks as identity theft and fraud. The extension of the mandatory breach notification to the public sector will strengthen the protection of privacy legislation in Alberta.

Recommendation:

- Require public bodies to report privacy incidents meeting certain criteria to my Office and giving me the power to require public bodies to notify affected individuals.

OTHER MATTERS

I would like to provide the following recommendations in addition to my comments on the themes raised in the *Discussion Guide*.

Annual reporting

Currently, public bodies provide statistical reports to Service Alberta regarding the number of access requests received in a fiscal year, the exemptions applied, and the timelines for response. Service Alberta subsequently publishes these statistics in an annual report. However, I do not believe the annual statistics reported by Service Alberta provide a comprehensive picture of compliance.

Recommendation:

- Consider implementing a monitoring and reporting model similar to the one under the Government of India's *Right to Information Act, 2005* (Chapter VI, section 25). Under this model, public bodies would submit annual reports to my Office that would include information such as:

    - the number of access requests received by the public body;
    - the timelines for response and the decisions to refuse or grant access;
    - fees charged or waived;
    - the number of time extensions taken by public bodies on their own initiative;
    - the number of breach incidents – description of incidents and steps undertaken by public bodies in relation to the incidents;
    - educational initiatives undertaken to inform the public as to their access and privacy rights;
    - educational initiatives undertaken to inform employees and contractors of public bodies of their obligations under the FOIP Act.

Review of paramountcy provisions

Paramountcy provisions remove access and privacy rights. As Commissioner Work stated in this Office's 2011 study of paramountcy clauses that override the FOIP Act:[15]

> *Left unchecked, the practice of taking other enactments out of FOIP by making them "paramount" to FOIP has the potential to turn FOIP into "a piece of Swiss cheese" , causing its death "by a thousand cuts" or bringing about its virtual "repeal by degrees."* [Introduction]

A number of existing paramountcy provisions may be unnecessary as the FOIP Act provides sufficient privacy protection. A mandatory requirement that proposed paramountcy provisions be submitted to me for review and comment can help in reducing the number of unnecessary paramountcy provisions.

Paramountcy provisions should also be reviewed periodically to determine ongoing relevancy and necessity. This FOIP Act Review is an excellent opportunity to revisit the existing paramountcies over the FOIP Act.

Recommendation:

- Require that all current paramountcy provisions be reviewed for necessity as part of this FOIP Act Review, that any future proposed paramountcy be submitted to my Office for review and comment, and that sunset clauses be included in all paramountcy provisions.

[15] http://www.oipc.ab.ca/Content_Files/Files/Publications/Report-ParamountProvisions.pdf

SUMMARY OF RECOMMENDATIONS

1. Making the FOIP Act clear and user friendly

- Review the scope of the FOIP Act to ensure that publicly-funded entities that should be captured are. Confirm the ongoing need for exclusions**.**

- Review the exceptions to access set out in the FOIP Act to ensure they are as narrow and limited as possible.

- Review the wording of the FOIP Act with an eye to making it more "plain-language" and understandable for the public and stakeholders.

- Ensure adequate resources are allocated to providing educational resource materials for both the public and stakeholders (e.g. Frequently Asked Questions and Bulletins produced by Service Alberta). Develop and provide cost-effective FOIP training options.

- Review the current fee requirements to ensure that fees are appropriate and not a barrier to access.

- Review current fee schedules to ensure they are clear and understandable.

- Before making any decision or recommendation to separate the two parts of the Act, it is important to clearly identify the objective that is to be achieved and how separating the Act would achieve it. A thorough cost-benefit analysis should also be undertaken.

2. Open Government and the FOIP Act

- Amend the FOIP Act to require public bodies to identify categories of records that will be made publicly available without requiring formal access requests. Require public bodies to make these records available.

- Establish minimum standards for proactive disclosure to provide guidance to public bodies and consistency to the public. Minimum standards could include:

  - specifying in legislation certain categories of records that public bodies must make available, such as: expenses, contracts over a certain dollar value, audit reports, etc.

  - requiring public bodies to establish publication schemes that identify classes of records that will be made available, methods by which the information will be made accessible, fees (if any) that may be charged, and how the public body will make the publication scheme available to the public. Consider requiring public bodies to submit publication schemes to my Office (or alternatively, a government ministry) for review and comment.

- Consider amending the FOIP Act to include a duty for public bodies to publish responses to general access requests. Develop minimum standards to ensure consistency and that information that could potentially be harmful is not released.

- Require public bodies to complete and submit AIAs to my Office on proposed

initiatives, schemes or programs that meet certain criteria (e.g. information sharing initiatives, data matching initiatives).

- Ensure appropriate statutory and policy framework for records and information management is in place to support transparency, accountability and compliance with the FOIP Act. This could include amending the FOIP Act to require that public bodies:

  - create such records as are reasonably necessary to document their decisions, actions, advice, recommendations and deliberations.

  - ensure that all records are covered in records retention and disposition schedules

3. Sharing personal information to provide programs and services

- Proposed information sharing initiatives must be thoroughly reviewed and assessed for access and privacy implications before implementation to determine whether or not they are required. This includes ensuring that any legislative amendments are harmonized among the FOIP Act, HIA and PIPA to avoid introducing inconsistencies.

- Dedicate resources to education, training and resource materials.

- Include a requirement in the FOIP Act that all cross-sectoral information sharing initiatives be registered with my Office or a designated government ministry. The registry listing could document the nature of the information sharing initiative, names of participating stakeholders, and contact information of an officer/employee who can answer questions about the collection, use, disclosure, retention, security or destruction of personal/health information. The registry should be regularly updated and easily accessible to the public.

- Legislative schemes authorizing information sharing without consent must ensure that all participants are subject to Alberta's information and privacy laws.

- Include a requirement in the FOIP Act that public bodies must conduct and submit privacy impact assessments to my Office for information sharing initiatives that involve data matching and for any cross-sectoral initiatives.

- Stakeholders participating in cross-sectoral information sharing initiatives should be required to record disclosures, including disclosures via information systems, comparable to section 41 and section 41(1.1) of the HIA:

  - the name of the person/service provider to whom the information was disclosed;
  - the date and purpose of the disclosure; and
  - a description of the information disclosed.

- Legislation should ensure that individuals who are the subject of the information sharing have an express right to ask for access to and a copy of the disclosure notes. Individuals should also have a right to ask me for a review in relation to their requests (similar to section 41(3) of HIA).

4. Addressing technological innovation

- Require public bodies to complete and submit privacy and access impact assessments to my Office on proposed initiatives, schemes or programs that meet certain criteria (for example, information sharing initiatives as discussed above).

- Require public bodies to report privacy incidents meeting certain criteria to my Office and giving me the power to require public bodies to notify affected individuals.

Other matters

- Consider implementing a monitoring and reporting model similar to the one under the Government of India's *Right to Information Act, 2005* (Chapter VI, section 25). Under this model, public bodies would submit annual reports to my Office that would include information such as:

    - the number of access requests received by the public body;
    - the timelines for response and the decisions to refuse or grant access;
    - fees charged or waived;
    - the number of time extensions taken by public bodies on their own initiative;
    - the number of breach incidents – description of incidents and steps undertaken by public bodies in relation to the incidents;
    - educational initiatives undertaken to inform the public as to their access and privacy rights;
    - educational initiatives undertaken to inform employees and contractors of public bodies of their obligations under the FOIP Act.

- Require that all current paramountcy provisions be reviewed for necessity as part of this FOIP Act Review, that any future proposed paramountcy be submitted to my Office for review and comment, and that sunset clauses be included in all paramountcy provisions.