Office of the Information and
Privacy Commissioner of Alberta

November 30, 2020

Honourable Nate Glubish
Minister of Service Alberta
103 Legislature Building
10800 – 97 Avenue NW
Edmonton, AB T5K 2B6

Dear Minister Glubish:

I have appreciated our previous meetings and discussions about the *Freedom of Information and Protection of Privacy Act* (FOIP Act) and the *Personal Information Protection Act* (PIPA). In my office's Annual Report 2019-20, I committed to writing to ask you to consider updates to these important pieces of legislation.

The recommendations I am putting forward at this time were selected with a view to adapting the legislation to reflect accelerated digitization in all sectors in light of the COVID-19 pandemic and enhanced societal expectations relating to access to information and privacy rights.

With respect to potential amendments to the FOIP Act, I recommend amendments that would further digitize the freedom of information system, improve information sharing for effective and efficient service delivery, modernize privacy protections and accountability mechanisms, strengthen oversight, reduce court burdens, improve the time extensions process, and ensure regular legislation reviews. The FOIP Act recommendations are attached as Appendix A. I have also attached a copy of my 2013 submission with recommendations for technical amendments, titled *Making the FOIP Act Clear, User-Friendly & Practical* (Appendix D).

With respect to potential amendments to PIPA, my recommendations are meant to enhance accountability measures, better enable the use of de-identified personal information for innovation and research, give consumers more choice by enhancing business competition, strengthen oversight, and build public trust in personal information practices by expanding the scope of the law. PIPA recommendations are attached as Appendix B.

My office most recently made recommendations to amend PIPA during the 2016 legislative review (Appendix E). Much has changed in private sector privacy law since that time.

There have been significant changes in 2020 alone. Quebec introduced Bill 64 in June, which proposes sweeping amendments to both public and private sector laws, and is undergoing extensive public consultation. The federal government introduced Bill C-11 on November 17, which proposes an overhaul to the *Personal Information Protection and Electronic Documents Act*. Ontario launched a public consultation in August with the aim to introduce its own private sector privacy law. Finally, British Columbia's PIPA was under review by a special parliamentary committee prior to their provincial

election. The national discussions and proposed changes notably reflect many principles in the European Union's *General Data Protection Regulation*, which came into force in 2018.

Of all of these, the changes proposed in Bill C-11 require careful consideration as they may affect PIPA's "substantially similar" standing federally. My office is continuing to monitor Bill C-11, as it may lead to further recommendations for PIPA.

I would like to note that the recommendations I have highlighted in the attached appendices are not exhaustive, and I believe both Acts deserve comprehensive reviews by a special committee of the Legislative Assembly. Over the past several years, public scrutiny of access and privacy laws has increased, and the COVID-19 pandemic has intensified the spotlight on access and privacy rights. These realities reinforce the need for a guided public consultation on how to improve the FOIP Act and PIPA. Public reviews by a special committee of the Legislative Assembly would allow my office and all stakeholders to engage in meaningful and helpful discussions on improving the laws.

In light of my annual report commitment to write to you about modernizing the FOIP Act and PIPA, and to talk openly about my ideas for improvement, I will be making this letter and attachments public.

Thank you again for your attention and commitment to the access and privacy rights of Albertans. I look forward to further discussing with you and your staff efforts to modernize the FOIP Act and PIPA.

Sincerely,

[Original signed by Jill Clayton]

Jill Clayton
Information and Privacy Commissioner

cc: Cynthia Farmer, Deputy Minister, Service Alberta
29th fl ATB Place South, 10020 - 100 Street, Edmonton, AB, T5J 0N3

Appendix A: FOIP Act Recommended Improvements

1. Information Sharing

In order to facilitate the use of data for societal benefits, modern access to information laws need to allow the government to pool data sources to facilitate management or allocation of resources, planning for the delivery of programs and services, and the evaluation of those programs and services.

Ontario recently enacted amendments to their *Freedom of Information and Protection of Privacy Act* (Part III.1: Data Integration) which allow for the creation of data integration units within and outside of public bodies. The Ontario approach facilitates data pooling across government but builds numerous protections including data minimization, de-identification requirements, approval of data standards by the Commissioner, written agreements, privacy impact assessment requirements, mandatory breach reporting, and regular reviews of policies and processes by the Commissioner.

Recommendation: The FOIP Act adopt the Ontario approach for information sharing.

2. Modern Privacy Protections

In order to adequately protect the privacy interests of citizens in the era of artificial intelligence (AI) and big data, there are two fundamental privacy protections missing from the FOIP Act:

- **Mandatory Privacy Impact Assessments (PIAs):** A PIA is an important tool for ensuring that any new project or program is privacy compliant. A PIA helps a public body identify and mitigate the privacy risks associated with the collection, use or disclosure of personal information. In the increasingly complex world of big data, PIAs have become essential.

  Under the *Health Information Act*, it is mandatory for health custodians to submit PIAs to the OIPC for review and comment before implementing a new initiative. It is not mandatory for public bodies under the FOIP Act to prepare or submit a PIA to my office, although public bodies occasionally submit PIAs voluntarily.

  As former Commissioner Work noted in the 2010 FOIP Review, the intent of mandatory PIAs is not to impose a burden on public bodies but to assure Albertans that a public body has fulfilled its due diligence and its statutory obligation under the FOIP Act to protect the privacy of Albertans.

  Recommendation: The FOIP Act be amended to require public bodies to complete and submit to the Commissioner privacy impact assessments for all information sharing initiatives (as noted above), where the public body is developing an information system or an electronic service delivery project, or where the public body plans to disclose personal information without consent or to disclose personal information outside of province.

- **Mandatory Privacy Breach Reporting:** Perhaps nothing is more fundamental to building trust in citizens than breach notification. Governments have the ability to collect an enormous amount of personal information about individuals. Citizens have the right to know that public bodies are managing personal information entrusted to them appropriately, and to protect themselves

against such risks as identity theft and fraud when their personal information has been compromised.

Furthermore, privacy breaches are often an important learning experience for the public body and breach reporting to me ensures that all the necessary steps are taken and prevention lessons are learned.

Mandatory breach reporting is required for private-sector organizations under PIPA and for health custodians under the *Health Information Act.* The extension of the mandatory breach notification to the public sector will strengthen the protection of privacy legislation in Alberta and enhance public trust in government.

Recommendation: The FOIP Act be amended to include mandatory notification of a privacy breach to an individual and to the Commissioner where there is a real risk of significant harm to the individual as a result of the loss or unauthorized access or disclosure of personal information, with the associated powers for the Commissioner that exist in PIPA.

3. Access Rights – Electronic Format for Responsive Records

It is becoming increasingly common for access laws to require disclosure of records in an electronic format, when requested by the applicant.

Considering societal expectations of information access and delivery and government's increased storage of information in electronic formats, this requirement would streamline access request processing for government and applicants alike.

Recommendation: The FOIP Act be amended to require that, upon request, information supplied in response to an access request be released electronically to an applicant using a structured, commonly used technological format.

4. Access Rights – Time Extensions

The COVID-19 pandemic further highlights a practical issue relating to the permitted time extensions for responding to an access request.

Section 14(1) of the FOIP Act allow a public body to grant itself a 30-day extension for responding to an access request in specified circumstances. If a public body requires an extension longer than the additional 30 days, it must submit a time extension request to me for approval.

However, the circumstances specified in section 14(1) do not include unforeseen or extenuating circumstances, such as the current pandemic, the 2013 closure of the Alberta Records Centre due to structural concerns, or wildfires or floods that have affected municipal operations. Therefore, public bodies have no authority to grant themselves a 30-day extension under section 14(1) if they are unable to access records in these situations. Furthermore, I have no authority to grant time extensions under section 14(1) in these situations.

In contrast, British Columbia's *Freedom of Information and Protection of Privacy Act,* section 10(2)(b), allows the BC Commissioner to grant the head of a public body permission to extend the time for responding if the Commissioner "otherwise considers that it is fair and reasonable to do so,

as the commissioner considers appropriate." This permitted the BC Commissioner to grant public bodies additional time to process access requests as a result of the pandemic and public health emergency.

Recommendation: The FOIP Act be amended to allow the head of a public body to extend the time for responding to an access request for up to 30 days, or, with the Commissioner's permission, for a longer period in unforeseen emergency or disaster situations.

In addition, there are a number of technical amendments required to section 14 that would provide greater clarity to the understanding and operation of the time extension provisions. These are outlined in my *Making the FOIP Act Clear, User-friendly & Practical* submission to the 2013 government review of the FOIP Act (attached as Appendix D).

5. Strengthening Oversight – Solicitor-Client Privilege Material

As noted above, modern access and privacy laws are being strengthened to ensure that oversight is meaningful and effective.

As I outlined in my April 2017 special report to the Legislative Assembly of Alberta, entitled *Producing Records to the Commissioner* (Appendix F), the operation of the FOIP Act and my ability to perform my functions as an Officer of the Legislature under that Act have been compromised by my inability to require public bodies to give me records for which public bodies are claiming solicitor-client privilege or related privileges, such as litigation privilege.

The FOIP Act grants me the power to review a public body's response to an access request, including determining whether exceptions to disclosure have been properly applied. Currently, when an exception to disclosure for solicitor-client privilege (or other related privileges) is questioned by my office because adequate evidence has not been provided to support the claim, the power to make the decision regarding the claimed privilege is transferred to the courts.

In my view, this approach has several disadvantages by:

- Increasing resources of the Court at a time when those resources are stretched to the limit;
- Requiring that the Court have an expedited process to avoid lengthy delays (i.e. it currently takes a year to get before the Court on judicial reviews of my decisions);
- Increasing the cost for public bodies, my office and citizens;
- Requiring multiple decision makers in a single case, as well as multiple appeal routes, unduly complicating and protracting the process; and
- Requiring judges of the Court appointed as Adjudicators under section 75 of the FOIP Act to follow this same procedure, as Adjudicators appointed under section 75 have only those powers that I have under the FOIP Act.

Recently Canada's antiquated *Access to Information Act* was updated to clarify and support the Commissioner's right to review records subject to claims of solicitor-client privilege. The purpose is simply to ensure that access to information rights are subject to meaningful and timely review.

Recommendation: The FOIP Act be amended to state explicitly that:

- The Commissioner has the power to require public bodies to produce to the Commissioner records over which solicitor-client privilege and other similar privileges (e.g. litigation privilege, informer privilege) are claimed;
- The Commissioner may require those records when, in the Commissioner's opinion, it is necessary to perform the Commissioner's functions (such as when a public body does not provide enough evidence to satisfy me that the records are privileged);
- Solicitor-client privilege or other legal privilege is not waived when the privileged records are provided to the Commissioner; and
- The Commissioner may not disclose to the Minister of Justice and Solicitor General, as evidence of an offence, records to which solicitor-client privilege applies.

6. Offences – Limitation Period for Prosecution

Currently, a prosecution of an offence under the FOIP Act must be commenced within 2 years after the commission of the alleged offence.

Offences are prosecuted by the Crown. However, the FOIP Act permits me to disclose to the Minister of Justice and Solicitor General information relating to the commission of an offence if I consider there is evidence of an offence. Occasions have arisen where the current 2-year limitation period has already expired when evidence of a possible offence is discovered by my office.

The *Health Information Act* currently contains a limitation period for the prosecution of certain offences of 2 years after the day on which evidence of the alleged offence first came to the attention of the Commissioner, but not afterwards. Bill 46, introduced in the Legislative Assembly on November 5, 2020, proposes to extend this limitation period to all offences under the *Health Information Act*.

Recommendation: That section 92(5) of the FOIP Act be amended to state that a prosecution of an offence under the Act be commenced within 2 years after the day on which evidence of the alleged offence first came to the attention of the Commissioner, but not afterwards.

7. Review of the Act

The FOIP Act is an act of general application of significant importance to Albertans. Legislating a commencement date or time period for subsequent reviews of the Act ensure that the legislation remains current and relevant. Not specifying a commencement date or time period for a review leaves the review of the legislation to the will of the government of the day and puts the legislation at risk for not meeting the access to information and privacy needs of Albertans.

Historically, section 97 of the FOIP Act was amended after a review of the Act by a special committee of the Legislative Assembly to indicate the commencement of the next review. In the November 2010 Final Report to the Legislative Assembly, the reviewing Standing Committee recommended that section 97 be amended to provide for a further review of the Act in six calendar years. Unfortunately, no amendments followed the 2010 Final Report, with the result that the FOIP Act has not had a comprehensive review by a special committee of the Legislative Assembly for a decade.

Recommendation: Section 97 of the FOIP Act be amended to require that a special committee of the Legislative Assembly must begin a comprehensive review of the Act and the regulations made under it

(a) by a specified date in 2021, and
(b) thereafter, every 6 years after the date on which the previous special committee submits its final report to the Legislative Assembly, and
(c) that a special committee must submit its final report to the Legislative Assembly within 12 months after beginning a review.

Appendix B: PIPA Recommended Improvements

1. Privacy Management Programs

Increasingly businesses – big and small – are adapting rapidly to provide services to customers online. Businesses engaged in any part of the digital economy must ensure that they comply with all of the various privacy laws that affect them as they conduct business. Privacy management programs are technical and organizational measures to ensure that organizations plan ahead and build privacy into new products and services. This reduces privacy breaches and the costs associated with them. Increasingly laws require these programs and so, in many jurisdictions interprovincial and international business can no longer be conducted without them. Privacy management program requirements exist in GDPR and are proposed in Quebec's Bill 64 and the federal Bill C-11.

Recommendation: PIPA be amended to require organizations to have a privacy management program in place and that organizations provide written information about their privacy management program to the Commissioner and to individuals, upon request. The requirements of a privacy management program should be adaptable and scalable to the size of the organization and to the volume and sensitivity of the personal information that is in its custody or under its control.

Other aspects that could make up part of the requirement to establish a privacy management program include:

- **Mandatory Privacy Impact Assessments (PIAs):** Require PIAs for projects meeting certain criteria. For example, see the *General Data Protection Regulation's* Article 35 on Data Protection Impact Assessments.
- **Automated Decision-Making:** Require that organizations:
    - Disclose if they are using automated decision-making system to make predictions, recommendations or decisions about individuals that could have significant impacts on them;
    - Require that organizations provide meaningful information about the logic involved, significance and consequences;
    - Add a right for individuals to object to automated decision-making; and
    - Add a right for individuals who object to automated decision-making to have the objection be evaluated by an individual, so that individuals are not subject to a decision that produces legal effects based solely on automated processing.

2. Innovation and Research

Modern privacy laws incentivize responsible innovation. Economically and socially beneficial innovation is good for businesses and citizens. It is virtually impossible, however, to foresee all future insights derived from personal information collected for AI or other types of big data projects and possible uses that may be made of it. Unknown risks associated with inherent algorithmic bias and potential downstream discriminatory harms are difficult to anticipate, let alone address, which has led to recent focus on ethical assessments of big data initiatives.

A broader approach to innovation and research could allow for the pooling of de-identified personal information from more than one organization using a "data trust". For example, Ontario uses "prescribed entities" under its health privacy law to facilitate the pooling and sharing of data. These

entities are subject to special oversight including a regular review of their policies and procedures by the privacy commissioner.

Recommendation: That the government explore data trusts as a potential enabler of responsible innovation. At minimum, PIPA be amended to:

- Permit the use of de-identified personal information without consent for internal research and development purposes;
- Define "de-identified" to mean to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual; and
- Add an offence for attempting to re-identify individuals using de-identified information.

3. Scope

Non-commercial entities such as non-profit organizations and political parties process significant amounts of often highly personal information, but not all non-profit organizations and no political parties are subject to PIPA. If sensitive personal information is worthy of protection then it must be protected no matter what entity holds the information.

With respect to non-profit organizations, previous legislative committees have recommended that all non-profit organizations be subject to PIPA, as they are in British Columbia. There are inconsistencies with how PIPA applies to non-profit organizations. As we move towards better enabling multi-sector information sharing projects and socially beneficial innovations, it is important to ensure consistency in how privacy laws apply to the project partners involved. The lack of statutory privacy protection causes confusion and delays, and may result, for example, in hesitancy to share personal information with or receive personal information from non-profit organizations that are not subject to privacy law.

With respect to political parties, certain activities exposed publicly have negatively affected public trust in the personal information practices of political parties. Only British Columbia's laws fully capture the personal information collected, used and disclosed by political parties. Canada's Privacy Commissioners joined together in October 2018 calling for enhanced protections of citizens in their interactions with political parties. The addition of political parties to PIPA's scope would help to secure privacy and trust in our electoral process.

Recommendation: PIPA be amended to make the Act apply fully to all non-profit organizations and political parties.

4. Individual Rights – Data Portability

At the heart of privacy laws is the principle that individuals have a right to control their own personal information. Control of personal information has grown increasingly complex in the digital world. Three new rights have emerged under modern privacy laws to address this complexity, including the:

- Right to erasure
- Right to de-indexing
- Right to data portability

All three are important rights and worth consideration. Of the three, the right to data portability is the most straightforward and has gained the most support nationally and internationally.

The right to data portability would give individuals the right to extract all of their data from a business or organization and transfer it in a structured, readily useable, standardized format to a different platform that offers a similar service. This right would engender competition by facilitating the ability of individuals to transfer their data between commercial entities. This is good for business and good for citizens.

Recommendation: PIPA be amended to include the right to data portability. In addition, the government should conduct further consultations on the right to erasure and the right to de-indexing.

5. Strengthen Oversight and Penalties

Privacy regulation requires a variety of strategies to ensure compliance. The majority of organizations understand that consumer trust is paramount. Compliance with privacy laws builds trust and is good for business.

As seen around the world, however, some organizations require greater motivations to comply with the law. Jurisdictions around the globe have therefore strengthened the oversight and penalty regimes in public, health and private sector laws. These strengthened measures include giving privacy regulators the ability to administer monetary penalties and increasing the fines for offences.

There are elements of privacy protection that are so fundamental that serious, repetitive or long-term infractions require significant penalties. An administrative monetary penalty regime would make clear that the privacy rights of Albertans are meaningful and well protected. In addition, fines for offences in Alberta are currently well below the proposed fine structures in Quebec's Bill 64 and the federal Bill C-11. The very existence of a regime that includes administrative monetary penalties and significant penalties for offences would act as a sufficient deterrent that few penalties would be imposed.

Recommendation: PIPA be amended to strengthen oversight and offence and penalty provisions as follows:

- **Administrative Monetary Penalties**: PIPA be amended to:
    - Grant the Commissioner power to impose administrative monetary penalties for listed violations including such things as failure to report a privacy breach, failure to notify about and provide an opportunity to object to automated decision making, and failure of security safeguards;
    - Require that the Commissioner develop and publish general administrative monetary penalty rules; and
    - Set the penalties at a level intended to deter non-compliance consistent with other jurisdictions.

- **Increase Offence Fines:** PIPA be amended to update the fine structure to bring Alberta in line with other Canadian jurisdictions.

Appendix C: Summary of FOIP Act and PIPA Recommendations

Freedom of Information and Protection of Privacy Act

Recommendations include that the FOIP Act be amended to:

1. Adopt the Ontario approach for information sharing.

2. Require public bodies to complete and submit to the Commissioner privacy impact assessments for all information sharing initiatives, where the public body is developing an information system or an electronic service delivery project, or where the public body plans to disclose personal information without consent or to disclose personal information outside of province.

3. Include mandatory notification of a privacy breach to an individual and to the Commissioner where there is a real risk of significant harm to the individual as a result of the loss or unauthorized access or disclosure of personal information, with the associated powers for the Commissioner that exist in PIPA.

4. Require that, upon request, information supplied in response to an access request be released electronically to applicant using structured, commonly used technological format.

5. Allow the head of a public body to extend the time for responding to an access request for up to 30 days, or, with the Commissioner's permission, for a longer period in unforeseen emergency or disaster situations.

   In addition, there are a number of technical amendments required to section 14 that would provide greater clarity to the understanding and operation of the time extension provisions. These are outlined in *Making the FOIP Act Clear, User-friendly & Practical* submission to the 2013 government review of the FOIP Act.

6. State explicitly that:

   - The Commissioner has the power to require public bodies to produce to the Commissioner records over which solicitor-client privilege and other similar privileges (e.g. litigation privilege, informer privilege) are claimed;
   - The Commissioner may require those records when, in the Commissioner's opinion, it is necessary to perform the Commissioner's functions (such as when a public body does not provide enough evidence to satisfy me that the records are privileged);
   - Solicitor-client privilege or other legal privilege is not waived when the privileged records are provided to the Commissioner; and
   - The Commissioner may not disclose to the Minister of Justice and Solicitor General, as evidence of an offence, records to which solicitor-client privilege applies.

7. State in section 92(5) that a prosecution of an offence under the Act be commenced within 2 years after the day on which evidence of the alleged offence first came to the attention of the Commissioner, but not afterwards.

   Require in section 97 that a special committee of the Legislative Assembly must begin a comprehensive review of the Act and the regulations made under it

(a) by a specified date in 2021, and
(b) thereafter, every 6 years after the date on which the previous special committee submits its final report to the Legislative Assembly, and
(c) that a special committee must submit its final report to the Legislative Assembly within 12 months after beginning a review

Personal Information Protection Act

Recommendations include that the PIPA be amended to:

1. Require organizations to have a privacy management program in place and that organizations provide written information about their privacy management program to the Commissioner and to individuals, upon request. The requirements of a privacy management program should be adaptable and scalable to the size of the organization and to the volume and sensitivity of the personal information that is in its custody or under its control.

   Other aspects that could make up part of the requirement to establish a privacy management program include:

   - **Mandatory Privacy Impact Assessments (PIAs):** Require PIAs for projects meeting certain criteria.
   - **Automated Decision-Making:** Require that organizations:

     - Disclose if they are using automated decision-making system to make predictions, recommendations or decisions about individuals that could have significant impacts on them;
     - Require that organizations provide meaningful information about the logic involved, significance and consequences;
     - Add a right for individuals to object to automated decision-making; and
     - Add a right for individuals who object to automated decision-making to have the objection be evaluated by an individual, so that individuals are not subject to a decision that produces legal effects based solely on automated processing.

2. That the government explore data trusts as a potential enabler of responsible innovation. At minimum, PIPA be amended to:

   - Permit the use of de-identified personal information without consent for internal research and development purposes;
   - Define “de-identified” to mean to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual; and
   - Add an offence for attempting to re-identify individuals using de-identified information.

3. Make the Act apply fully to all non-profit organizations and political parties.

4. Include the right to data portability. In addition, the government should conduct further consultations on the right to erasure and the right to de-indexing.

5. Strengthen oversight and offence and penalty provisions as follows:

- **Administrative Monetary Penalties**: PIPA be amended to:

    - Grant the Commissioner power to impose administrative monetary penalties for listed violations including such things as failure to report a privacy breach, failure to notify about and provide an opportunity to object to automated decision making, and failure of security safeguards;
    - Require that the Commissioner develop and publish general administrative monetary penalty rules; and
    - Set the penalties at a level intended to deter non-compliance consistent with other jurisdictions.

- **Increase Offence Fines:** PIPA be amended to update the fine structure to bring Alberta in line with other Canadian jurisdictions.

Appendix D: ***Making the FOIP Act Clear, User-Friendly & Practical*** **(July 2013)**

MAKING THE FOIP ACT CLEAR, USER-FRIENDLY & PRACTICAL

Submission to the 2013
Government of Alberta
FOIP Act Review

Office of the Information and
Privacy Commissioner of Alberta

In my submission to the 2013 FOIP Act Review, *Becoming a Leader in Access and Privacy,* I provided ideas, suggestions and recommendations for consideration in making Alberta's *Freedom of Information and Protection of Privacy Act* (the FOIP Act) a leading example to other jurisdictions in terms of access to information and protection of privacy legislation. In this second submission, I make comments and recommendations on technical aspects of the FOIP Act.

This submission responds to the theme "Making the FOIP Act Clear and User Friendly" that was raised in the *Discussion Guide* prepared by Service Alberta for the FOIP Act Review. I have, however, expanded the theme to "Making the FOIP Act Clear, User Friendly & Practical". It is important that legislation be written in clear and understandable terms. However, it is equally important that legislation be written to ensure that it can be applied practically.

As I said in *Becoming a Leader in Access and Privacy,* my Office has interpreted, mediated, investigated and issued orders, reports and decisions on hundreds of matters under the FOIP Act over the past 17 years. Our work and experiences have provided us with knowledge of the FOIP Act that is unique and comprehensive. In particular, we have an understanding of the practical application of the FOIP Act.

The FOIP Act is a good law and it has served Albertans well for the past 17 years. The current FOIP Act Review provides an opportunity to clarify and make amendments, as required, to strengthen and enable the FOIP Act to address the access to information and privacy issues of today's environment.

In releasing *Becoming a Leader in Access and Privacy*, I said that I hoped my Office would be consulted during the next phases of the FOIP Act Review and provided an opportunity to comment on any proposed amendments to the FOIP Act. I would like to reiterate this comment as I believe my Office has extensive knowledge of the FOIP Act and its application to the public sector.

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

CONTENTS

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act* (the FOIP Act) applies to over 1,000 "public bodies," including:

- government ministries, boards and agencies;
- universities and colleges;
- school boards and charter schools;
- health care bodies; and
- local government bodies such as:

    - police services,
    - police commissions,
    - municipalities,
    - metis settlements,
    - improvement districts,
    - housing management bodies,
    - library boards, and
    - any board, committee, commission, panel, agency or corporation created or owned by a local government body and all members or officers are appointed or chosen by the local government body.

Given the breadth of the application of the FOIP Act and the diverse range of expertise and knowledge of the legislation by public bodies, it is essential that the FOIP Act be clear, understandable and practical in application.

GENERAL RECOMMENDATIONS

Cross-sectoral partnerships

There is an increasing movement towards citizen-centred service delivery involving cross-sectoral partners (public, private and health sectors). I am concerned that the personal information of Albertans may not be protected in situations where one of the partners is a non-profit organization that is not subject to privacy legislation.

Public bodies are accountable under the FOIP Act for the collection, use and disclosure of personal information by their "employees".

Health custodians are subject to the *Health Information Act* (HIA) and private sector organizations are subject to the *Personal Information Protection Act* (PIPA).

However, only certain non-profit organizations are fully subject to PIPA. Non-profit organizations that are incorporated under the *Societies Act* or the *Agricultural Societies Act,* or are registered under Part 9 of the *Companies Act*, are subject to PIPA only when they are collecting, using or disclosing personal information in connection with a commercial activity. It should be noted that in its 2007 Final Report, the all-party Select Special PIPA Review Committee recommended that all non-profit organizations be fully subject to PIPA.

If such a non-profit organization is a partner in a multi-partner service program, is not providing a service on behalf of a public body (e.g. as a contractor) and is not undertaking a commercial activity, the collection, use and disclosure of personal information by the organization would not be protected by privacy legislation.

The Standing Committee on Health (the Standing Committee) considered this issue in its 2010 review of the FOIP Act. In its Final Report to the Legislature, the Standing Committee recommended that the definition of "employee" under section 1(e) of the FOIP Act be amended to read:

> *…"employee", in relation to a public body includes a person who performs a service for or in relation to or in connection with the public body as an appointee, volunteer or student or under a contract or agency relationship with a public body.*

On reflection, I do not believe that the recommendation is an appropriate solution. In my opinion, the best solution is to make all non-profit organizations fully subject to PIPA, as recommended by the 2007 Select Special PIPA Review Committee. In the meantime, a provision should be added to the FOIP Act making the public body responsible for the acts of the non-profit organization with respect to personal information that is shared between them when they are partners in a program or service.

Recommendation:

- Amend the FOIP Act to establish that when public bodies and non-profit organizations that are not subject to PIPA are sharing personal information as partners in cross-sectoral initiatives, the public bodies are responsible for the collection, use, disclosure and protection of that personal information by the non-profit organizations.

Section 14(1) – extending time limit for responding

Section 11(1) of the FOIP Act requires that public bodies respond to an access/correction request no later than 30 calendar days after receiving the request. However, the 30-day time limit may be extended under section 14.

Under section 14(1), a public body may grant itself an additional 30-day extension in certain circumstances. If a public body requires an extension longer than the additional 30 days, it must submit an extension request to me for approval.

The circumstances under section 14(1) do not include unanticipated situations such as the recent flooding and recovery situation in Calgary or the closure of the Alberta Records Centre in February 2013 due to structural concerns.

Therefore, public bodies have no authority to grant themselves an additional 30-day extension under section 14(1) if they are unable to access records in these situations. Furthermore, I have no authority to grant time extensions under section 14(1) in these situations.

Recommendation:

- Amend section 14(1) to allow for extensions in unforeseen emergency or disaster situations.

Section 14(1) – time extensions that a public body can take on its own authority

Section 10(1) of the *Freedom of Information and Protection of Privacy Act* of British Columbia (BC) corresponds with Alberta's section 14(1).

However, the BC FOIP Act separates the additional 30-day extension that a public body may take on its own authority from the longer extensions that may be permitted by the Commissioner. This is different from section 14(1) of Alberta's FOIP Act which encompasses both the additional 30-day extension that a public body may take on its own authority and a longer extension that may be permitted by the Commissioner.

Separate provisions specific to extensions by public bodies and extensions by the Commissioner may provide greater clarity to public bodies that they may extend the time limits for response by an additional 30-day period on their own authority.

Recommendation:

- Amend section 14(1) to separate and clarify the extensions that a public body may take on its own authority from the longer extensions permitted by the Commissioner.

In addition, my Office has heard some public bodies interpret section 14(1) as permitting them to take a 30-day extension for each of the circumstances listed under section 14(1). For example: a public body may take one 30-day extension under section 14(1)(a) and another 30-day extension under section 14(1)(b). I believe this interpretation is contrary to the intent of the FOIP Act to ensure that requests are processed in a timely manner.

I prefer the wording in section 10(1) of the BC FOIP Act which states that a "public body may extend the time for responding to a request for up to 30 days if one or more of the following apply…".

Recommendation:

- Clarify that under section 14(1) a public body may only take one additional 30-day extension on its own authority.

Section 14(1)(c) and section 14(3) – third parties

Section 14(1)(c) allows the time limits for responding to an access/correction request to be extended if "more time is needed to consult with a third party or another public body before deciding whether to grant access to a record".

Section 14(3) states:

> 14(3) Despite subsection (1), where the head of a public body is considering giving access to a record to which section 30 applies, the head of the public body may extend the time for responding to the request for the period of time necessary to enable the head to comply with the requirements of section 31.

The consultation with a third party under section 14(1)(c) is different from the third party consultation process set out in section 14(3) of the FOIP Act which relates to sections 30 and 31.

In a footnote on page 4 of Order F2011-003, Commissioner Work stated:

> *Section 14(1)(c) refers to consultations with third parties. However, in my view, the third parties being referenced there are not those who may have interests under section 30(1), but rather are other third parties such as, for example, government organizations that are not public bodies under the Act.*

While the difference between section 14(1)(c) and section 14(3) was addressed in Order F2011-003, I believe it would be helpful to reinforce this in the FOIP Act. For instance, the reference to "a third party" in section 14(1)(c) could be replaced with other wording such as "another government, organization or agency" or words of that nature.

Recommendation:

- Amend section 14(1)(c) to replace "a third party" with other wording to minimize confusion with section 14(3).

Additionally, as noted above, section 14(3) relates to section 30 and section 31. The wording in sections 30 and 31 refers to "the record or part of the record". However, section 14(3) only refers to "the record". Since these provisions are related, the wording should be consistent to avoid confusion or misinterpretation.

Recommendation:

- Amend section 14(3) to read "where the head of a public body is considering giving access to a record **or part of a record** to which section 30 applies…".

Section 14(1)(d) – third party requests a review

Section 14(1)(d) allows a public body to extend the time limits for response on its own authority or with my permission if "a third party asks for a review under section 65(2) or 77(3)".

When a third party asks me for a review under section 65(2) of the FOIP Act, the timelines for that review are set out in section 69(6) of the FOIP Act. Under section 69(6), I am required to complete my review within 90 days after receiving the request for review unless I extend that time. Since a public body has limited say in the timelines required for completion of my review, the intent of section 14(1)(d) is unclear.

The 2009 edition of the *FOIP Guidelines and Practices* [page 65], prepared by Service Alberta, provides the following information about section 14(1)(d):

> *In order to allow time for the third party to ask the Commissioner to review the decision, an additional 20 days may be required…*

Section 65(2) of the FOIP Act gives a third party that has been notified under section 31 of a decision by a public body to release third party information the right to ask me to review that decision. Under section 66(2)(b), a third party must submit their request to me within 20 days after they are notified of the decision.

The 20-day period is also referenced in section 31(3) of the FOIP Act, which states that a public body must give written notification to both the third party and the applicant of its decision to give the applicant access to third party information, unless the third party asks for a review within 20 days after that notice is given.

In my opinion, there is a difference between allowing time for a third party to ask for a review (as stated in the *FOIP Guidelines and Practices*) and the wording of section 14(1)(d) which is "a third party asks for a review" (which implies that the third party request for review has been made to me).

Furthermore, as stated in Order F2011-003:

> *Sections 30/31 create a separate procedure and requirements for responding for a specific category of records – those which it is considering disclosing but which affect or may affect third party interests. This is necessary because for this latter category of records, access is not to be given despite a public body's decision to disclose, because the affected third parties must be given an opportunity to request a review by my office of the public body's decision before the records are actually released in accordance with the decision.* [para 11]

The requirements and timelines under section 30 and section 31 are mandatory. Public bodies are required to notify third parties and applicants as to the requirements and timelines. Given this, it may make sense to have a provision that states that the time limits for response to an applicant's request, in relation to records that affect or may affect third party interests, would be extended when a third party asks for a review (as opposed to an extension that is taken by a public body on its own authority or with permission from me). However, whether this provision is under section 14(1) or elsewhere in the FOIP Act should be reviewed. This provision must only be specific to the records that are the subject of the third party review. Release of records not related to the third party interests should not be delayed.

Recommendation:

- Consider the appropriate place for a provision stating the time limits for response in relation to records that affect or may affect a third party's interests are extended when a third party asks for a review.

Section 14(1) – time extensions taken by the OIPC as a public body

The Office of the Information and Privacy Commissioner (the OIPC) is a "public body" and subject to the FOIP Act except for records that are excluded under section 4(1)(d).

When the OIPC receives an access to information request for records that are not excluded under section 4(1)(d), I am required to respond in accordance with the time limits set out in section 11 and section 14.

Under section 14(1), as the head of the OIPC, I may take an additional 30-day extension (similar to other public bodies). As stated above, if public bodies require an extension that is longer than the additional 30-day period, they may come to me for permission and I issue my decision. However, there is no provision under section 14(1) that allows me to ask for an extension beyond the additional 30-day period.

Under section 75 of the FOIP Act, the Lieutenant Governor in Council may designate a judge of the Court of Queen's Bench of Alberta as an adjudicator on decisions or actions made by me as the head of the OIPC. I will make further comments about an adjudicator under section 75 later in my submission. But, at this point, I will describe the adjudicator's role in relation to my Office as similar to my role as Commissioner for other public bodies. Therefore, it seems reasonable that I would need to write to the adjudicator for extensions beyond the additional 30-day period. Currently, there is nothing under section 75 that relates to this matter.

It should also be noted that I cannot submit a time extension request unless an adjudicator is appointed – a process that can take more than 30 days. Consequently, there is a gap in the FOIP Act on this matter.

Recommendation:

- Clarify how time extensions beyond the additional 30-day period for the OIPC as a public body be handled.

Section 14(4)(c) – complaints about extensions

Section 14(4)(c) states that an applicant is to be informed of the right to make a complaint to "the Commissioner or to an adjudicator" about any time extensions taken with respect to their access/correction request.

Because of the wording in section 14(4)(c), this section may be interpreted to mean that when the Commissioner grants a public body permission to extend time for a response longer than 30 days, that decision is reviewable by an adjudicator. As explained below, this is incorrect.

An "adjudicator" is defined in section 1(a) of the FOIP Act as "a person designated under section 75," i.e. a judge of the Court of Queen's Bench who has been designated by Order in Council to act as the Commissioner in specified circumstances.

An adjudicator under section 75 reviews my decisions and actions when I am acting as the head of the OIPC as a public body. An adjudicator cannot review the decisions I make in my role as Commissioner; as expressly stated in section 75(2), an adjudicator "must not review an order of the Commissioner made under this Act."

The proper forum for review of my decisions as Commissioner is by way of application for judicial review to the Court. This is supported by the decision in *Alberta (Information and Privacy Commissioner) v. Alberta (Freedom of Information and Protection of Privacy Act Adjudicator)*, 2011, ABCA 36, where the Court of Appeal of Alberta stated:

> *[81]….I prefer the analysis of Smith J. of the British Columbia Superior Court acting as adjudicator in Mr. M. in which she held at para. 9:*
>
> > *The Commissioner has two distinct roles under the Act: (1) overseeing and administer the Act, and (2) acting as head of a public body. It is only the acts or omissions by the Commissioner in the latter capacity that are subject to review by an adjudicator. This is an important distinction because the bulk of the Commissioner's work, which includes monitoring compliance by other public bodies, investigating complaints and promoting public awareness of the Act, is subject only to judicial review and is not reviewable by an adjudicator…*

When I am reviewing a public body's request for an extension, I am acting as Commissioner and not as the head of a public body. Therefore, any decision to grant or deny a public body's request

for a time extension under section 14 of the FOIP Act is not a matter that can be reviewed by an adjudicator under section 75. As stated in the Court of Appeal of Alberta decision, the correct forum to hear this matter is judicial review.

However, when I, as head of the OIPC, take the permitted 30-day time extension in section 14(1) for an access request that has been made to the OIPC as a public body, I must comply with section 14(4)(c), as any other public body must, and inform the applicant that he or she has the right to make a complaint about the time extension. In this case, the complaint is to an adjudicator because I cannot act as Commissioner and review decisions I have made as head of a public body.

It is the Commissioner who reviews complaints about a public body's decision to grant itself a 30-day time extension on its own authority.

Recommendation:

- Amend section 14(4)(c) to clarify that an applicant's complaint about a decision of a public body to grant a time extension on its own authority is to be made to the Commissioner (unless the public body is the OIPC).

Section 30(5) – notice to applicant

Both sections 30 and 31 of the FOIP Act require that public bodies provide notice to applicants and third parties.

Section 30(1) and section 31(2) states that notices to the third party must be in writing. Section 31(3) also states that notice to the applicant must be in writing. However, there is no requirement that a notice to an applicant under section 30(5) must be in writing. This provision should be amended for consistency and clarity.

Recommendation:

- Amend section 30(5) to state that a notice to the applicant under this provision must be in writing.

Section 31 – release of third party records

Under section 31(3), a public body must wait 20 days after notice has been given to a third party and an applicant of its decision to disclose *before* it can release records to the applicant. This 20-day period allows a third party time to ask me for a review under section 65(2) of the public body's decision to disclose.

During the 2010 FOIP Act Review, the Standing Committee heard that this 20-day period is unnecessary in circumstances where the third party has consented to the disclosure and where there is no additional third party affected by the disclosure.

The Committee made the following recommendation in its November 2010 report:

> *That section 31 of the FOIP Act be amended to state that the 20-day requirement under section 31(3) does not apply when a third party has consented to the disclosure and the disclosure would not impact another third party.*

I would like to reiterate this recommendation to facilitate the timely release of records under the FOIP Act.

Recommendation:

- Amend section 31(3) in accordance with the recommendation of the Standing Committee on the 2010 FOIP Review.

Section 66 – how to ask for a review

Under section 66(2)(a)(i) of the FOIP Act, an individual must deliver their written request for review to the Commissioner within 60 days after being notified of a public body's decision. The difficulty with requesting a review pursuant to section 65(3) is that there is often no notification of a decision from a public body regarding a privacy breach. Furthermore, individuals may not realize their privacy has been breached until some time has elapsed from the actual incident.

Separating the time limits for submitting a privacy complaint from the 60-day period set out in section 66(2)(a)(i) with a provision similar to section 47(3) of the *Personal Information Protection Act* (PIPA) is a possible solution. Section 47(3) of PIPA reads:

> 47(3) A written complaint to the Commissioner about an organization must be delivered within a reasonable time.

Recommendation:

- Amend section 66(2) to require written complaints be delivered to my Office within a reasonable time.

Section 68 – mediation may be authorized

Section 68 gives me the discretion to authorize "a mediator" to investigate and try to settle any matter that is the subject of a request for review.

The intent of section 68 is to allow for dispute resolution outside of the formal adjudication process. The majority of matters that come to my Office are successfully resolved without requiring an inquiry or an order.

Section 68 encompasses both mediation and investigation, which are different types of dispute resolution. However, the header to this section only refers to mediation and the title of "mediator" does not include the investigative role that my staff may be required to fulfill.

For clarity, I suggest the wording of section 68 be amended to more accurately reflect the informal dispute resolution process in my Office.

Recommendation:

- Amend section 68 to reflect the informal dispute resolution process of my Office.

New provision – Commissioner's refusal to conduct or continue a review

Section 49.1 of PIPA allows me the discretion to refuse to conduct or continue a review in the following circumstances:

- the written request for review is frivolous or vexatious or is not made in good faith, or
- the circumstances warrant refusing to conduct or to continue a review.

I am mindful of the principles and rights set out in the FOIP Act. However, there are individuals who may use the FOIP Act in ways that are contrary to the spirit and intent of the law. The Legislature has recognized this in section 55(1) of the FOIP Act, which allows a public body to ask me for authorization to disregard certain requests.

I must ensure that my limited resources are allocated to matters that are proper and in accordance with the intentions of the Act.

Recommendation:

- Add a new provision to the FOIP Act similar to section 49.1 of PIPA.

Section 69(6) – time limit on reviews by the Commissioner

Section 69(6) requires that a review by my Office be completed within 90 days after receiving the request for review unless I extend that time limit.

In its November 2010 Final Report to the Legislature, the Standing Committee said:

> *…even if the Commissioner had unlimited resources, it would not be possible to complete a mediation/investigation, conduct an inquiry and issue an order within 90 days of receiving a request for review. When a matter goes to inquiry, the parties must be notified, providing them time to prepare their submissions, which are then provided to the Commissioner's office. Then the Commissioner must prepare and issue his decision. The Committee heard that this entire process requires more time than the 90 days allocated under section 69(6)…*

The Standing Committee recommended:

> *That section 69(6) of the FOIP Act be amended to match the one-year time limit in PIPA, with the ability to extend if required.*

Recommendation:

- Amend section 69(6) in accordance with the recommendation of the Standing Committee on the 2010 FOIP Review.

Division 2, Part 5 – clarifying the adjudicator's role relative to the Commissioner's legislative oversight role

As mentioned earlier in this submission, the Commissioner has two distinct roles which have been recognized by the Court of Appeal of Alberta: (1) overseeing and administering the FOIP Act, and (2) acting as head of a public body, i.e. the OIPC.[1]

As stated in section 75(2), an adjudicator is not permitted to review an order of the Commissioner made under the FOIP Act. It is only decisions, acts or failures to act by the Commissioner in her capacity as head of a public body that are subject to review by an adjudicator, not the decisions, acts or omissions that relate to the Commissioner's legislative oversight role.
In its November 2010 Final Report, the Standing Committee recommended:

> *That Division 2, Part 5, be amended to clarify that any decision, act or failure to act by the Commissioner in relation to his or her legislative oversight role is not reviewable by an adjudicator appointed under section 75.*

Recommendation:

- Amend Division 2, Part 5 in accordance with the recommendation of the Standing Committee on the 2010 FOIP Review.

[1] *Alberta (Information and Privacy Commissioner) v. Alberta (Freedom of Information and Protection of Privacy Act Adjudicator)*, 2011, ABCA 36

Section 84(1)(e) – exercise of rights by other persons

There is no minimum age specified in the FOIP Act. Therefore, children have rights similar to adults under the FOIP Act. In cases where a child is a minor, section 84(1)(e) of the FOIP Act permits the head of a public body to allow a guardian to exercise the minor's rights.

However, section 84(1)(e) does not contemplate the exercise of a minor's rights with respect to requesting a review by the Commissioner of a public body's decision regarding an access or correction request or improper collection, use or disclosure of personal information. In these situations, it is the Commissioner, not the head of a public body, that would permit a guardian to exercise the minor's right to request a review or file a complaint. The addition of the word "Commissioner" to section 84(1)(e) would clarify this matter.

In addition, consideration should be given to amending section 84(1)(e) to reflect the concept of a "mature minor", similar to section 104(1)(b) and (c) of the *Health Information Act* (HIA).

Recommendations:

- Amend section 84(1)(e) to include reference to "the Commissioner."
- Consider amending the section further to reflect the concept of a "mature minor," similar to HIA.

Section 97 – review of the FOIP Act

In its November 2010 Final Report to the Legislature, the Standing Committee recommended:

> *That section 97 of the FOIP Act be amended to provide for a further review of the Act in six calendar years.*

The FOIP Act is an act of general application of significant importance to Albertans. Legislating a commencement date or time period for subsequent reviews of the Act ensures that the legislation remains current and relevant. Not specifying a commencement date or time period for review leaves the review of the legislation to the will of the government of the day and puts the legislation at risk for not meeting the access to information and privacy needs of Albertans.

Recommendation:

- Amend section 97 of the FOIP Act in accordance with the recommendation of the Standing Committee on the 2010 FOIP Review.

RECOMMENDATIONS FOR HARMONIZATION WITH PIPA AND HIA

The following recommendations are to harmonize the FOIP Act with PIPA and HIA:

- Incorporate a provision, similar to section 38.1 of PIPA, into section 56 of the FOIP Act. Section 38.1 of PIPA states:

  > 38.1 If a legal privilege, including solicitor-client privilege, applies to information disclosed to the Commissioner on the Commissioner's request under section 37.1 or section 38, the legal privilege is not affected by the disclosure.

- Add a provision, similar to section 39(1.1) of PIPA, to section 57 of the FOIP Act. Section 39(1.1) of PIPA reads:

  > 39(1.1) The Commissioner and anyone acting for or under the direction of the Commissioner shall not give or be compelled to give evidence in a court or in any other proceeding in respect of any information obtained in performing their duties, powers and functions under this Act, except in the circumstances set out in subsection (1(a) to (c).

- Add a provision, similar to section 41(3.2) of PIPA, to section 59 of the FOIP Act. Section 41(3.2) of PIPA states:

  > 41(3.2) The Commissioner shall not disclose information under subsection (3.1) if the information is subject to solicitor-client privilege.

- Amend section 72(3)(a) to read the same as section 52(3)(a) of PIPA, which states:

  > Confirm that a duty imposed by this Act or the regulations has been performed or require that a duty imposed by this Act or the regulations be performed.

- Add the word "excuse" to section 72(3)(c), similar to section 52(3)(c) of PIPA:

  > Confirm, **excuse** or reduce a fee or order a refund, in the appropriate circumstances, including if a time limit is not met.

- Add a new provision under section 72(3) that is similar to section 52(3)(f) of PIPA, which states:

  > Confirm a decision of an organization to collect, use or disclose personal information.

- Add a provision similar to section 52(2)(b) of PIPA to section 72 of the FOIP Act. Section 52(2)(b) of PIPA allows me to:

  > Make an order that the Commissioner considers appropriate if, in the circumstances, an order under section 52(2)(a) would not be applicable.

- Delete section 74(5) for consistency with PIPA.

- Amend section 92 to remove the word "wilfully" from the offence provisions and to create a due diligence defence. The same amendments were made to the offence provisions in PIPA in 2010.

SUMMARY OF RECOMMENDATIONS

General recommendations

- Amend the FOIP Act to establish that when public bodies and non-profit organizations that are not subject to PIPA are sharing personal information as partners in cross-sectoral initiatives, the public bodies are responsible for the collection, use, disclosure and protection of that personal information by the non-profit organizations.

- Amend section 14(1) to allow for extensions in unforeseen emergency or disaster situations.

- Amend section 14(1) to separate and clarify the extensions that a public body may take on its own authority from the longer extensions permitted by the Commissioner.

- Clarify that under section 14(1) a public body may only take one additional 30-day extension on its own authority.

- Amend section 14(1)(c) to replace "a third party" with other wording to minimize confusion with section 14(3).

- Amend section 14(3) to read "where the head of a public body is considering giving access to a record **or part of a record** to which section 30 applies…".

- Consider the appropriate place for a provision stating the time limits for response in relation to records that affect or may affect a third party's interests are extended when a third party asks for a review.

- Clarify how time extensions beyond the additional 30-day period for the OIPC as a public body be handled.

- Amend section 14(4)(c) to clarify that an applicant's complaint about a decision of a public body to grant a time extension on its own authority is to be made to the Commissioner (unless the public body is the OIPC).

- Amend section 30(5) to state that a notice to the applicant under this provision must be in writing.

- Amend section 31(3) in accordance with the recommendation of the Standing Committee on the 2010 FOIP Review.

- Amend section 66(2) to require written complaints be delivered to my Office within a reasonable time.

- Amend section 68 to reflect the informal dispute resolution process of my Office.

- Add a new provision to the FOIP Act similar to section 49.1 of PIPA.

- Amend section 69(6) in accordance with the recommendation of the Standing Committee on the 2010 FOIP Review.

- Amend Division 2, Part 5 in accordance with the recommendation of the Standing Committee on the 2010 FOIP Review.

- Amend section 84(1)(e) to include reference to "the Commissioner."

- Consider amending the section further to reflect the concept of a "mature minor," similar to HIA.

- Amend section 97 of the FOIP Act in accordance with the recommendation of the Standing Committee on the 2010 FOIP Review.

Recommendations for harmonization with PIPA and HIA

- Incorporate a provision, similar to section 38.1 of PIPA, into section 56 of the FOIP Act. Section 38.1 of PIPA states:

  > 38.1 If a legal privilege, including solicitor-client privilege, applies to information disclosed to the Commissioner on the Commissioner's request under section 37.1 or section 38, the legal privilege is not affected by the disclosure.

- Add a provision, similar to section 39(1.1) of PIPA, to section 57 of the FOIP Act. Section 39(1.1) of PIPA reads:

  > 39(1.1) The Commissioner and anyone acting for or under the direction of the Commissioner shall not give or be compelled to give evidence in a court or in any other proceeding in respect of any information obtained in performing their duties, powers and functions under this Act, except in the circumstances set out in subsection (1(a) to (c).

- Add a provision, similar to section 41(3.2) of PIPA, to section 59 of the FOIP Act. Section 41(3.2) of PIPA states:

  > 41(3.2) The Commissioner shall not disclose information under subsection (3.1) if the information is subject to solicitor-client privilege.

- Amend section 72(3)(a) to read the same as section 52(3)(a) of PIPA, which states:

  > Confirm that a duty imposed by this Act or the regulations has been performed or require that a duty imposed by this Act or the regulations be performed.

- Add the word "excuse" to section 72(3)(c), similar to section 52(3)(c) of PIPA:

  > Confirm, **excuse** or reduce a fee or order a refund, in the appropriate circumstances, including if a time limit is not met.

- Add a new provision under section 72(3) that is similar to section 52(3)(f) of PIPA, which states:

  > Confirm a decision of an organization to collect, use or disclose personal information.

- Add a provision similar to section 52(2)(b) of PIPA to section 72 of the FOIP Act. Section 52(2)(b) of PIPA allows me to:

  > Make an order that the Commissioner considers appropriate if, in the circumstances, an order under section 52(2)(a) would not be applicable.

- Delete section 74(5) for consistency with PIPA.

- Amend section 92 to remove the word "wilfully" from the offence provisions and to create a due diligence defence. The same amendments were made to the offence provisions in PIPA in 2010.

Appendix E: *Review of the Personal Information Protection Act* (February 2016)

Review of the Personal Information Protection Act

Submission to the Standing Committee on Alberta's Economic Future

February 2016

Office of the Information and Privacy Commissioner of Alberta

On June 15, 2015, the Legislative Assembly of Alberta designated the Standing Committee on Alberta's Economic Future (Committee) as a special committee tasked with conducting a comprehensive review of the *Personal Information Protection Act* (PIPA) pursuant to section 63 of the Act. As part of its review, the Committee issued a *Discussion Guide*, opened a consultation process, and invited feedback from stakeholders.

I am pleased to make this submission to the Committee, which contains ideas, suggestions and recommendations for PIPA. This report's purpose is to ensure Alberta remains a leader in private sector privacy legislation across Canada and internationally.

Jill Clayton
Information and Privacy Commissioner of Alberta
February 2016

Contents

Introduction

The Office of the Information and Privacy Commissioner (OIPC) welcomes this opportunity to share its experiences regarding the administration of the *Personal Information Protection Act* (PIPA) with the Standing Committee on Alberta's Economic Future (Committee).

Albertans should be proud of this private sector privacy legislation. PIPA reflects its made-in-Alberta approach, as it came into force only after extensive consultation with Albertans and organizations to ensure that privacy compliance would not be onerous for small- and medium-sized businesses, yet would ensure the rights of Albertans to have their personal information protected. The Supreme Court of Canada has characterized PIPA as "quasi-constitutional", emphasizing the important role of this legislation in preserving our free and democratic society.[1]

Over the past decade, there has been a growing awareness among Albertans that they have the right to control their personal information. Albertans understand laws are in place which protect their personal information and give them rights of access. Organizations, generally, also have a better understanding of their duties to protect the personal information in their custody and control.[2]

Since PIPA's proclamation in 2004, there have been staggering changes in technology. The magnitude of personal information being collected by organizations around the globe, as well the ease with which it is used and disclosed, is unprecedented. It is an unfortunate fact that personal information data breaches now make headlines on a daily basis. While the repercussions of each data breach vary from mildly annoying to very serious, they all affect individuals. Everyone knows someone who has been affected by a breach, whether they are neighbours, colleagues, friends, family members or themselves.

PIPA Stats

From January 1, 2004 (when PIPA came into force) to December 31, 2015:

- 126 Orders/Decisions
- 26 Investigation Reports
- 3,138 files opened and 2,853 files closed
- 91% of files that could go to inquiry were resolved at the mediation stage
- 20% of the total OIPC caseload
- 60% of the total general inquiries (telephone calls)

Alberta has been a leader, both nationally and internationally, for its approach to private sector privacy. As a result of the last PIPA Review, Alberta became the first jurisdiction in Canada to require mandatory breach reporting in 2010. PIPA continues to serve as a model for other jurisdictions contemplating similar provisions.

A body of jurisprudence has also built around the interpretation of PIPA. Orders/Decisions and Investigation Reports provide guidance to individuals and organizations in understanding how PIPA works.

In addition, a generally consistent body of jurisprudence has been developed by other jurisdictions with substantially similar legislation. The Commissioner has worked closely with

1 *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19.

2 These trends were explored in detail in the OIPC's *General Population Survey Final Report* and the *Stakeholder Survey Report* available at www.oipc.ab.ca.

the oversight offices for federal and British Columbia private sector privacy laws to harmonize approaches to privacy protection. For example, in 2011 the Privacy Commissioner of Canada and the Alberta and British Columbia Information and Privacy Commissioners signed the *Memorandum of Understanding with Respect to Co-operation and Collaboration in Private Sector Privacy Policy, Enforcement and Public Education*.[3] The three offices have also jointly published numerous resources, such as *Getting Accountability Right with a Privacy Management Program*.[4]

Not only is PIPA generally consistent with similar legislation across Canada, but historically, Alberta has seen benefit in attempting to harmonize, to the extent it is reasonable, the rules for privacy protection between Alberta's three primary statutes: PIPA, the *Health Information Act*[5] (HIA), and the *Freedom of Information and Protection of Privacy Act*[6] (FOIP Act). There is interplay among these three statutes: a significant number of employees in Alberta routinely deal with more than one of these laws in the course of their work. Using common terms, concepts and tests simplifies to a great extent the rules for collection, use and disclosure and ultimately improves statutory compliance by those many workers subject to these laws. Simplification and standardization also makes these laws more accessible to Albertans.

PIPA was designed to be technologically neutral – it requires organizations to consider the ways in which they collect, use and disclose personal information, regardless of the technological means chosen by those organizations. Despite the complexity of technological changes, PIPA has been and remains an effective law. It achieves an appropriate balance between protecting the privacy interests of Albertans and the legitimate collection, use and disclosure of their personal information by organizations for the purpose of providing goods and services. PIPA's continuing effectiveness is due, in part, to the wisdom of having a mandatory comprehensive review by a special committee of the Legislative Assembly every six years (section 63(1)(b)).

> *"The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy… legislation which aims to protect control over personal information should be characterized as 'quasi-constitutional' because of the fundamental role privacy plays in the preservation of a free and democratic society..."*
>
> - Supreme Court of Canada, *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19.

The work of the Committee is very important. The Committee faces the challenge of making reasonable adjustments to PIPA to maintain its relevance without thwarting its objectives or making the legislation unduly complicated. The OIPC is pleased to provide this submission with recommendations to improve PIPA.

---

3 *Memorandum of Understanding with Respect to Co-operation and Collaboration in Private Sector Privacy Policy, Enforcement and Public Education,* https://www.priv.gc.ca/au-ans/prov/mou_e.asp.

4 *Getting Accountability Right with a Privacy Management Program,* https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf.

5 *Health Information Act,* RSA 2000, c. H-5.

6 *Freedom of Information and Protection of Privacy Act*, RSA 2000, C. F-25.

Non-Profit Organizations

In its 2007 Final Report, the all-party MLA Select Special PIPA Review Committee recommended that PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year limitation period.[7]

The OIPC supported the Committee's recommendation and continues to maintain its long-held position that all not-for-profit organizations should be fully subject to PIPA, as they are in British Columbia.

As noted in the previous PIPA review, the definition of non-profit organization in PIPA "has resulted in different treatment of similar organizations under PIPA (i.e. not-for-profit organizations that fall within the definition and those that do not). This, in turn, has resulted in differences in the way these organizations treat the personal information of their clients, employees, volunteers, and donors."[9]

Under PIPA, a non-profit organization is defined as an organization that is:

- incorporated under the *Societies Act* or the *Agricultural Societies Act*; or
- registered under Part 9 of the *Companies Act* (section 56).

These non-profit organizations have to comply with PIPA only when they collect, use or disclose personal information in connection with a commercial activity. This means that if the personal information of clients, donors, volunteers and employees was not collected, used or disclosed by the non-profit organization in connection with a commercial activity, the organization does not have to:

- advise individuals of the purposes for which it is collecting information;
- limit the amount of personal information it is collecting;
- make a reasonable effort to ensure the personal information it is using is accurate and complete for the particular purpose;
- make a reasonable effort to safeguard the information (e.g. store it in a secure place and ensure that the information is seen only by persons within the organization that have a need to know);
- destroy the information in a secure manner or render it non-identifying when it is no longer reasonably required for legal or business purposes;
- notify the OIPC of a privacy breach where there is real risk of significant harm to individuals; or
- grant individuals access to their own personal information held by the organization, to correct that information, or to tell them how it is using the information and to whom it has been disclosed.

Moreover, the organization's clients, donors, volunteers and employees do not have the right to complain to the Commissioner about the improper collection, use, disclosure or security of their personal information by the organization, or to ask the Commissioner to review the organization's response to their request for access to their personal information. The Commissioner

7 *Select Special Personal Information Protection Act Review Committee, Final Report* (November 2007) at p. 10.

8 Ibid.

also cannot require the organization to notify affected individuals of a privacy breach that presents a real risk of significant harm to the individuals.

There are 18,884 active societies under the *Societies Act*, 295 active agricultural societies under the *Agricultural Societies Act* and 2,125 active non-profit companies under Part 9 of the *Companies Act*.[9]

Not-for-profit organizations that do not fall within the section 56 definition of "non-profit organization" are fully subject to PIPA. These include religious societies, housing cooperatives, unincorporated associations, federally incorporated not-for-profit organizations, and organizations incorporated by private Acts. These not-for-profit organizations have the same obligations under PIPA as other organizations and businesses in Alberta to protect the personal information in their custody or under their control. Their clients, donors, volunteers and employees enjoy the same privacy protections and rights as the customers, clients and employees of businesses subject to the Act.

Additional inconsistencies arise for both the organization and individuals when a section 56 non-profit organization undertakes both commercial and non-commercial activities. For example, selling a membership or a fundraising list is a commercial activity. If a section 56 non-profit organization sells the personal information of its donors without their consent, the donors can submit a complaint to the Commissioner. However, the donors cannot complain if the organization publishes sensitive personal information about the donor without consent on its website.

Since PIPA was enacted, some 60 cases involving section 56 non-profit organizations have been brought to the OIPC; however, PIPA applied in only a handful of cases. In the remaining cases, the non-profit organization was not subject to PIPA because there was no commercial activity taking place. The Commissioner has not had jurisdiction in any of the self-reported privacy breaches sent to the OIPC by section 56 non-profit organizations. Yet, the privacy breaches suffered by these organizations are typical of those of other organizations, such as missing paperwork; computer system upgrades gone awry; and stolen unencrypted laptops containing sensitive personal information about many individuals, including banking and credit card information, criminal record checks, and social insurance numbers.

The increased emphasis by government on information sharing initiatives highlights the need to include all not-for-profit organizations under PIPA. Information sharing initiatives are frequently cross-sectoral, with a network of public, health, private and non-profit groups exchanging personal information for the delivery of services or programs. While public sector bodies, health custodians and private businesses are subject to privacy laws, the non-profit agencies will not be, if they fall within PIPA's definition of a non-profit organization and are not carrying out a commercial activity. However, many of these non-

9 Information retrieved from the Alberta Corporate Registry as of March 31, 2015 and from Alberta Agriculture and Forestry, http://www1.agric.gov.ab.ca/$Department/deptdocs.nsf/all/rsv14613

profit organizations are involved with vulnerable populations and handle very sensitive personal information about their clients. This is particularly true for those organizations providing social service or health programs, such as emergency shelters, drug or alcohol addiction counselling, and assistance programs for seniors and persons with disabilities. As the Commissioner has consistently stated, the benefits of information sharing should not come at the expense of privacy rights. All parties involved in information sharing initiatives should be regulated by privacy legislation and subject to the Commissioner's independent oversight.

The lack of statutory privacy protection may also impact service delivery as information sharing partners may be hesitant to share information with non-profit organizations that are not subject to privacy law.

There may be concerns that making PIPA apply to those non-profit organizations that are not currently subject to PIPA would add to their administrative burden. PIPA was originally developed with small- and medium-sized businesses in mind – to make informational privacy requirements easier to implement and comply with. If small- and medium-sized non-profit organizations were fully subject to PIPA, their obligations would be the same as for small- and medium-sized businesses. As was recommended in the previous PIPA review, implementation could be delayed one year to allow non-profit organizations to prepare for compliance. The OIPC is willing to work with Service Alberta to provide resources that would help non-profit organizations understand their obligations under the Act.

Recommendation

1. **That PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year transition period.**

Strengthening Accountability: Privacy Management Programs

Organizations subject to PIPA are responsible for personal information in their custody or under their control and are accountable for their compliance with PIPA. The "accountability principle" is one of the core privacy principles established by the Organisation for Economic Co-operation and Development (OECD) in 1980.[10] These privacy principles are the foundation for Canada's privacy laws, including PIPA and the federal *Personal Information Protection and Electronic Documents Act*[11] (PIPEDA).

PIPA was enacted with certain requirements to promote an organization's accountability. For example:

- organizations must designate one or more individuals to be responsible for ensuring the organization's compliance with the Act (section 5(3));
- organizations are required to develop and follow policies and practices that are reasonable to meet their obligations under the Act, and to make written information about those policies and procedures available upon request (section 6); and
- organizations must make reasonable security arrangements for personal information in their custody or under their control (section 34).

However, the privacy landscape has changed significantly since PIPA's enactment. Rapid advancements in technology allow individuals to share large amounts of personal information through social networks, e-mail, web logs, cell phone GPS signals, call detail records, Internet search indexing, digital photographs and wearable devices, and through online purchase transactions. Businesses (and governments) are able to collect, store and analyze vast amounts of data in ways never contemplated, to gather intelligence and identify trends to respond with better customer service, improved products and increased marketing. Privacy breaches have proliferated, with incidents often involving the personal information of thousands of individuals. And identity theft has become a real issue.

In this environment, individuals are much more aware of their right to control their own personal information and the importance of protecting it. They need and want to better understand how an organization is handling their personal information and what measures are in place to protect their privacy. This understanding is more critical when their information is being shared by partners in the private, public and health sectors for program or service delivery.

At the same time, organizations are more aware that personal information is one of the most valuable assets of an organization and that their business relies on maintaining the trust and confidence of their customers and employees by properly managing personal information. Organizations need a better understanding of how to build privacy and accountability into their operations – in short, how to implement a privacy management program that helps to minimize risks, strengthens privacy controls and supports compliance with their obligations under PIPA.

In their 2012 joint publication, *Getting Accountability Right with a Privacy Management*

10 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

11 *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5.

Program,[12] the Privacy Commissioners of Alberta, British Columbia and Canada provide guidance on what makes a strong privacy management program. The fundamentals include:

- appointing a person to be responsible for the development, implementation and maintenance of the privacy management program;
- developing and documenting internal policies that address the obligations under PIPA;
- educating and training employees in privacy protection;
- conducting privacy risk assessments;
- managing personal information handling by third party service providers;
- having systems in place to respond to individuals' requests for access to (and correction of) personal information or complaints about the protection of their information;
- having breach response and reporting protocols;
- informing individuals of their privacy rights and the organization's program controls; and
- monitoring, assessing and revising their privacy framework to ensure it remains relevant and effective.

The OECD has also recognized the importance of responsibility for compliance and revised its privacy guidelines in 2013 to include new provisions for implementing accountability within an organization. These provisions require the establishment of a privacy management program that:

- gives effect to the OECD Guidelines for all personal data under its control;
- is tailored to the structure, scale, volume and sensitivity of its operations;
- provides for appropriate safeguards based on privacy risk assessment;
- is integrated into its governance structure and establishes internal oversight mechanisms;
- includes plans for responding to inquiries and incidents; and
- is updated in light of ongoing monitoring and periodic assessment.

An organization must also be prepared to demonstrate its privacy management program to a data privacy enforcement authority, upon request.[13]

In its review of British Columbia's PIPA, the Legislative Assembly Special Committee agreed "that accountability is of critical importance to the effective implementation of PIPA" and recommended that organizations be required to adopt privacy management programs.[14]

The OIPC supports the implementation of privacy management programs by organizations. When

12 *Getting Accountability Right with a Privacy Management Program*, https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf.

13 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

14 *Report of Special Committee to Review the Personal Information Protection Act*, February 2015, at p. 11. The programs are to be tailored to the structure, scale, volume, and sensitivity of the operations of the organization; make the privacy policies of the organizations publicly available; include employee training; and be regularly monitored and updated. In a separate recommendation, the Committee supported mandatory breach reporting by organizations.

submitting privacy impact assessments (PIAs) to the OIPC for review,[15] health custodians, public bodies and private sector organizations are asked to describe the management and policy structure they have in place to ensure ongoing privacy compliance. Modernizing PIPA by explicitly requiring that organizations have a privacy management program in place will strengthen organizations' ongoing compliance with PIPA and will ensure PIPA remains current and harmonized with developments in accountability in other jurisdictions.

The requirements of a privacy management program should be adaptable and scalable to the size of the organization and to the volume and sensitivity of the personal information that is in its custody or under its control. An organization should also be prepared to demonstrate its privacy management program to individuals and to the Commissioner, upon request.

Recommendation

2. **That PIPA be amended to require that organizations have a privacy management program in place and that organizations provide written information about their privacy management programs to the Commissioner and to individuals, upon request.**

15 PIAs are prepared when new organizational practices or information systems are proposed that may affect the personal information of individuals. They are due diligence exercises that identify privacy concerns so they can be addressed before implementation of the new practice or system. PIAs are mandatory under the *Health Information Act*, but public bodies under the *Freedom of Information and Protection of Privacy Act* and private sector organizations may prepare and submit PIAs as a best practice.

Disclosures Without a Warrant

PIPA currently limits disclosures to law enforcement bodies without consent to circumstances where there is an investigation being undertaken with a view to a law enforcement proceeding or where such a proceeding is likely to result (section 20(f)).

PIPA also permits disclosures without consent where the disclosure is authorized or required by a statute or regulation of Alberta or Canada (section 20(b)), or if the disclosure is reasonable for an investigation or legal proceeding (section 20(m)). Both "investigation" and "legal proceeding" are defined in PIPA and require a breach of an agreement, a contravention of a law, or a remedy available at law – or for a breach, contravention or remedy to be likely to occur (sections 1(1)(f) and (g)).

These existing disclosure without consent provisions (and related definitions) narrow the circumstances in which an organization can disclose personal information without consent to law enforcement without a court order, warrant or subpoena. As discretionary provisions, they permit, but do not require, organizations to disclose personal information to law enforcement bodies. And in all instances, the disclosure must be only for purposes that are reasonable, and limited to what is reasonable for meeting those purposes (section 19).

The *Discussion Guide*[16] raised the question whether PIPA ought to be amended in response to the Supreme Court of Canada's decision in *R v. Spencer*[17] (*Spencer*), or to address the issue of warrantless disclosures more generally.

In *Spencer*, the Supreme Court of Canada considered whether police could request subscriber information from an internet service provider (ISP) for the purposes of a law enforcement investigation without a warrant. In that case, the Crown argued that the federal PIPEDA authorized the collection of the subscriber information by the police because it authorized the ISP to disclose that information to the police. The Supreme Court of Canada clarified that even if PIPEDA authorized the ISP to disclose the subscriber information, the police needed their own authority to collect that information. In other words, legislation such as PIPEDA and PIPA might authorize an organization to disclose personal information to law enforcement in certain circumstances, but that authority to disclose is not authority for the law enforcement body to collect the personal information.

Rather, the law enforcement body requires its own authority to collect the information. This authority may come from various places: a warrant or court order, the federal *Criminal Code*, or public sector privacy legislation, such as the FOIP Act in Alberta. However, the authority to collect cannot be found in legislation that governs private sector organizations, such as PIPA.

If there is a desire to amend legislation to limit collection of personal information by law enforcement, the appropriate place to do so is in legislation that directly governs those law enforcement bodies, such as the FOIP Act in Alberta. Other legislation like the *Criminal Code* is federal legislation that can only be amended by that level of government.

16 Standing Committee on Alberta's Economic Future, *Discussion Guide: The Personal Information Protection Act*, January 2016.

17 *R v. Spencer*, 2014 SCC 43.

Further, while concerns about the amount and extent of information disclosed by organizations to law enforcement are reasonable, organizations also have valid reasons for such disclosures, for example, reporting a possible crime or aiding an investigation. Not all collections of personal information by law enforcement require a warrant or court order; whether such a warrant or order is required will depend upon the circumstances of the collection and type of information being sought. It is the responsibility of the law enforcement body to know whether it is authorized to collect personal information from an organization (or any other source).

When considering a warrantless request from law enforcement for personal information, organizations should, as part of their due diligence, ask the law enforcement body to identify its authority for making the request.

PIPA's existing provisions for disclosure without consent to law enforcement bodies are working well. They provide organizations with the flexibility to protect personal information in their custody or under their control, and to disclose to law enforcement where circumstances call for doing so.

Recommendation

3. **That no changes be made to PIPA's disclosure without consent provisions pertaining to disclosures without a warrant.**

Transparency Reports

At its very core, PIPA balances the right of an individual to have his or her personal information protected and an organization's need to collect, use and disclose personal information for reasonable purposes.

An individual exercises control over his or her own personal information by deciding which organization can have his or her personal information and for what purposes. When organizations are able to collect, use or disclose that personal information for other purposes without consent, the loss of individual control is mitigated by an organization's obligation to be open, transparent and accountable for the personal information in its custody or under its control.

> *"[W]hile it can be confidently stated that governments are seeking and obtaining far more access to personal data contained in company hands than has formerly been the case, the precise extent of that access is somewhat unclear. It is within this context that transparency reporting may have a useful role to play."*
>
> - International Working Group on Data Protection in Telecommunications[18]

There has been an increasing reliance by government agencies,[19] and particularly law enforcement, on personal information collected by private businesses about their customers and clients. Information may be disclosed by the private organizations without consent as a result of judicial warrants or legislative requirements, to assist with investigations or emergency situations, or on a voluntary basis. Familiar examples of disclosures of customer or client information to law enforcement or government agencies include disclosures by telecommunications companies; disclosures by banks, money services businesses and real estate brokers to deter money laundering;[20] disclosures of patron information by Alberta bars to peace officers upon request;[21] and disclosures by pawnbrokers.[22]

The significant privacy concerns and lack of transparency around such disclosures has led to several recent initiatives:

- Some Canadian, US and global private sector organizations have begun publishing

18 *Working Paper on Transparency Reporting: Promoting accountability when governments access personal data held by companies* (April 2015) https://datenschutz-berlin.de/attachments/1118/675.50.14.pdf?1435752521.

19 See Office of the Information and Privacy Commissioner of Alberta, *Deputizing the Private Sector: Requiring the Collection of Personal Information by Non-Government Entities for Law Enforcement or Other Purposes*, May 2015 https://www.oipc.ab.ca/media/387467/report_deputizing_private_sector_may2015.pdf.

20 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17, http://laws-lois.justice.gc.ca/eng/acts/P-24.501/.

21 *Gaming and Liquor Act*, RSA 2000, c G-1; see also Office of the Information and Privacy Commissioner of Alberta and Alberta Gaming and Liquor Commission, *Guidelines for Licensed Premises: Collecting, Using and Disclosing Personal Information of Patrons* https://www.oipc.ab.ca/media/383672/guide_guidelines_for_licensed_premises_2009.pdf.

22 See *Business Watch International Inc. v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 10.

transparency reports voluntarily.[23]

- Since 2009, the Office of the Privacy Commissioner of Canada (OPC) has advocated for a reporting regime on personal information disclosures to government by commercial organizations. In 2015, the OPC issued a comparative analysis of transparency reporting by private sector companies.[24]
- In 2015, the Alberta OIPC commissioned an independent research paper, *Deputizing the Private Sector: Requiring the Collection of Personal Information by Non-Government Entities for Law Enforcement or Other Purposes*, to bring awareness to the subject.[25]
- In its 2014-15 review of British Columbia's PIPA, the Legislative Assembly Special Committee supported the position of the Information and Privacy Commissioner of British Columbia and recommended that organizations be required to document and publish transparency reports of disclosures made without consent.[26]
- In June 2015, Industry Canada (now Innovation, Science and Economic Development Canada) issued voluntary transparency reporting guidelines for private organizations.[27]
- In October 2015, the International Conference of Data Protection and Privacy Commissioner Offices issued a resolution calling on commercial organizations to maintain consistent records of government requests for access to customer and employee information and publish transparency reports outlining the number, nature and legal basis for those requests.[28]

PIPA requires organizations to be open and transparent about their policies and practices with respect to their management of the personal information of their customers, clients and employees (section 6). Organizations are also accountable for the personal information in their custody or under their control (section 5). While individuals have the right under PIPA to request information about how their personal information is and has been used by an organization and to whom it is being and has been disclosed (section 24(1.2)), there is no way for citizens in general, or the OIPC, to know the number, scale, frequency of, or reasons for disclosures without consent by private sector organizations to government or law enforcement agencies for non-business purposes. (By not knowing beforehand the frequency

23 Google www.google.com/transparencyreport; Apple http://www.apple.com/ca/privacy/transparency-reports/; Microsoft https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/; Rogers http://www.rogers.com/cms/pdf/en/2014-Rogers-Transparency-Report.pdf; Telus http://sustainability.telus.com/en/business_operations_and_ethics/governance_and_disclosure/transparency/; TekSavvy Solutions Inc. https://teksavvy.com/en/why-teksavvy/policies/legal-stuff/transparency-report; Sasktel http://www.sasktel.com/about-us/company-info/; MTS Allstream http://about.mts.ca/investors/governance/; Wind http://www.windmobile.ca/docs/default-source/default-document-library/2014-transparency-report-wind-mobileABF7DF074C25.pdf.

24 Office of the Privacy Commissioner of Canada, *Transparency Reporting by Private Sector Companies: Comparative Analysis* https://www.priv.gc.ca/information/research-recherche/2015/transp_201506_e.asp.

25 Ibid.

26 *Report of Special Committee to Review the Personal Information Protection Act*, February 2015.

27 See http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html.

28 See https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Transparency-Reporting.pdf.

with which their information is disclosed to government and law enforcement authorities, individuals are not able to make an informed decision as to whether to do business with that organization.)

Greater transparency and accountability in this area, as well as enhanced trust with customers and employees, would be achieved through periodic publication of transparency reports about disclosures to government and law enforcement agencies for non-business purposes. While some organizations may voluntarily publish transparency reports, prescribing the details of such reports ensures consistent and comparable data. The method of public reporting should be flexible to meet the nature of the organization's business; for example, reports could be posted on the organization's website.

Recommendation

4. **That PIPA be amended to address publication of transparency reports. Amendments should consider:**
   - **whether the reports should be limited to disclosures upon request of law enforcement or government agencies, or include disclosures made pursuant to legislation or on a voluntary basis;**
   - **the intervals for reporting; and**
   - **the minimum elements to be reported, such as the number and nature of the requests or disclosures, the legal authority for the request or disclosure, the response to requests (e.g. fulfilled, rejected, challenged), and the number of individuals or accounts involved.**

Freedom of Expression

In considering whether the current collection, use and disclosure provisions of PIPA that relate to trade unions are appropriate, it is important to keep in mind that PIPA does not limit expression except insofar as an organization uses individuals' personal information (without consent) – beyond this, PIPA has no effect on what trade unions may say.

In its decision in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, the Supreme Court of Canada said that PIPA had a defect which needed to be legislatively remedied. The defect was the absence of a mechanism for balancing a union's constitutional right of free expression with the privacy interests protected by PIPA.[29]

The Alberta Legislature amended PIPA in a way that balances trade unions' rights of free expression and individuals' privacy interests.

As part of this review of PIPA, parties may propose that particular categories of organizations (e.g. trade unions, but possibly other categories of organizations which called for similar expressive rights) be exempted from PIPA entirely.

If an exemption from the Act for any particular category of organization were put in place, the result would completely change the approach of the Act from one of prohibiting unauthorized collection, use and disclosure of personal information to one of removing any constraints for a particular category of organizations, leaving them free to collect, use or disclose any individual's personal information at will, regardless of any consequences to their privacy or to themselves.

If this course were taken, an individual whose information was collected, for example by a trade union, would have no mechanism (except possibly an injunction or a civil suit – though there is currently no tort of invasion of privacy recognized in Alberta) by which to ensure his or her personal information was collected, used and disclosed only for reasonable trade union purposes, having regard to the nature of the information, its sensitivity, and the potential of harm to the individual from its use and dissemination.

Similarly, an individual would have no way to ensure his or her personal information was used and/or further disseminated in a reasonable manner having regard to these same considerations. For example, it might not be reasonable to post highly sensitive personal information where it might permanently remain on the internet to achieve some relatively minor trade union purpose, or where the information was of minor importance in achieving that purpose; however, the individual whose information it was would have no way to prevent this nor any recourse if it happened.

Permitting such a result would not ensure proportionality between the expressive goals of the organization and the protection of the individual's privacy, such as was contemplated by the Supreme Court of Canada when it spoke of balancing these factors.

29 *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 25.

Another important consideration is that, if exempted, other provisions of PIPA would not apply to those organizations.

For example, once an organization has collected personal information, section 34 of PIPA imposes an obligation on the organization to safeguard that information against risks of unauthorized access, collection, use, disclosure, modification or destruction. Organizations must destroy information in a secure manner or render it non-identifying when it is no longer reasonably required for legal or business purposes (section 35).

Organizations are also required by PIPA to report privacy breaches to the Commissioner and ultimately to notify affected individuals where there is a real risk of significant harm to individuals as a result of the loss, or unauthorized access or disclosure of personal information in the organization's control (sections 34.1 and 37.1).

Under PIPA, individuals also have the right to request access to their own personal information held by an organization, to request correction of that information, and to ask how the organization is using their personal information and to whom it has been disclosed. They may ask the Commissioner to review the organization's response to their request and can complain to the Commissioner about the improper collection, use or disclosure of their personal information.

Exempting any particular category of organizations from PIPA would remove these important privacy protections for personal information in the custody or under the control of the exempted organization and eliminate the rights given to individuals under the Act.

The OIPC offers no view as to whether there are any other categories of organizations whose expressive rights merit special protection under the Act; any such organizations may identify themselves, and explain the circumstances under which their expressive rights should override the personal privacy interests of individuals.

Recommendation

5. **At this time, the OIPC is not recommending any additional changes to PIPA concerning freedom of expression. However, should the committee identify any organizations as needing a special provision for their expressive rights then the OIPC recommends those organizations should be included within the scope of a provision that provides for the balancing of the purposes of the expression with the privacy interests of individuals.**

Notification of a Breach of Privacy

PIPA requires organizations to protect personal information in their custody or control by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction (section 34). A privacy breach occurs when an organization's security arrangements fail, and there is an incident involving the loss of or unauthorized access to, or disclosure of personal information (section 34.1(1)).

Unfortunately, breaches involving personal information have become increasingly common over the last decade. In fact, on most days, some high-profile breach or another is widely reported in the media; many more breaches do not make headlines.

On May 1, 2010, as a result of the last PIPA Review, Alberta became the first jurisdiction in Canada to require organizations to report breaches to the Commissioner where there exists a "real risk of significant harm" to an individual as a result of the loss or unauthorized access to or disclosure of personal information (section 34.1(1)).

An individual who becomes a victim of a breach may be subject to a wide variety of "significant harms", including: identity theft, financial loss, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, negative effects on a credit record, damage to or loss of property, and even bodily harm.

A "real risk" means the likelihood that the harm will result is more than mere speculation or conjecture; there must be a cause and effect relationship between the breach incident and the possible harm. It is an offence for an organization to fail to report a personal information breach to the Commissioner where there is a real risk of significant harm to affected individuals (section 59(1)(e.1)). The Commissioner has the power to require an organization to notify affected individuals of the breach (section 37.1(1)).

The primary purpose of data breach notification and reporting is to ensure that affected individuals are informed of incidents so that they can take steps to protect themselves against harm. Breach notification also provides an incentive for organizations to implement and update safeguards for the personal information in their control.

Since PIPA's mandatory breach notification provisions came into force, the Commissioner has made publicly available all decisions where a real risk of significant harm was identified and notification to individuals was required. Some of the recent privacy breaches and trends discussed in the OIPC's 2014-15 Annual Report are highlighted below:

- **Human error** – this includes inappropriate storage or disposal of personal information, and emails or faxes sent to the wrong person.
- **Insider misuse of personal information** – although many organizations have reasonable security arrangements in place to protect personal information against outside threats, they remain vulnerable to internal threats. The best defence against insider misuse includes access controls that limit users' ability to access personal information to their business need to know, coupled with an audit program to ensure employees are following the organization's rules.
- **Malware, hacking and e-commerce** – Malicious software and hacking continues to be a significant cause of privacy breaches Recent breaches reported to the Commissioner by online retailers involved

credit card payment information being exposed to unknown parties over lengthy periods.

- **Social engineering** – this refers to deceiving users or administrators of computer systems into revealing confidential information.
- **Failure to wipe hard drives** – despite previous Investigation Reports and guidance from the Commissioner's office, too many organizations still do not pay proper attention to securely deleting media before it is disposed of or re-sold.

Generally, the breach notification provisions in PIPA appear to be working well. In practice, the Commissioner has found that many organizations have already notified, or are in the process of notifying affected individuals when they report a breach to the office under PIPA.

The number of reported breaches has increased over the last few years, although it is unknown whether this is due to an increase in the number of incidents, or better awareness of the duty to report to the Commissioner, (or, most likely, both). To date, since the provisions came into force, approximately 550 breaches have been reported to the Commissioner.

The Commissioner does not have jurisdiction over all of the breaches reported to the OIPC, and not all of the breaches reported to the Commissioner pose a real risk of significant harm. Some organizations may choose to report to the Commissioner out of an abundance of caution, or in cases where they are not sure whether there is a real risk of significant harm. The Commissioner reviews all reported breaches to assess whether the Commissioner has jurisdiction, and if so, whether notification is required. Approximately 54% of the reported breaches where the Commissioner has jurisdiction, pose a real risk of significant harm to affected individuals.

Alberta's PIPA has set an example for the rest of Canada. In the recent legislative reviews of British Columbia's PIPA, and the federal PIPEDA, recommendations were made to add breach reporting provisions similar to Alberta's. In particular, both regimes have set the breach reporting threshold to be the same as Alberta's: a "real risk of significant harm". PIPEDA's breach reporting provisions, outlined in the *Digital Privacy Act* [30], will come into effect once regulations are finalized. Organizations subject to PIPEDA will be required to notify individuals and report to the Commissioner all breaches where it is reasonable to believe the breach creates a real risk of significant harm to the individual. The recommendations made by British Columbia's Special Committee to Review PIPA have not yet been drafted into legislation.

As stated above, the breach notification provisions are working well; however, there is a recurring issue concerning the relationship between an organization and its service providers. Under PIPA, it is the organization with control of the personal information that is required to report a breach to the Commissioner, and ultimately notify individuals, of privacy breaches where the breach creates a real risk of significant harm to individuals. However, it is often the case that a service provider to the organization has personal information in its custody (e.g. outsourced payroll services) but not under its control.

30 *Digital Privacy Act*, S.C. 2015, c. 32

Control rests with the principal organization to which it is providing the service. Absent a contractual provision with an organization, service providers have no obligation to report a privacy breach to the principal organization when an incident occurs. This can result in the principal organization not finding out about a breach, or in some cases finding out about a breach long after it has occurred. In such cases, there is a delay in notification or no notification at all to the Commissioner and the individuals who are facing a real risk of significant harm.

A requirement under PIPA for service providers (those organizations with personal information in their custody but not their control), to report a breach to the organization with control of the personal information would resolve this issue. A similar amendment to HIA was included in the *Statutes Amendment Act, 2014* [31] where affiliates are required to notify custodians of any loss of or unauthorized access to or disclosure of individually identifying health information (provisions not yet in force).

Recommendations

6. **That PIPA be amended to require organizations having personal information in their custody to notify the organization having control of the same personal information, without unreasonable delay, of any incident involving the loss of or unauthorized access to or disclosure of personal information.**

7. **That the *PIPA Regulation* be amended to require organizations to provide information to the Commissioner about the relationship with a service provider when a service provider is involved in a breach incident.**

31 *Statutes Amendment Act, 2014*, S.A. 2014, c. 8

Solicitor-Client Privilege

Solicitor-client privilege has become a critically important issue before the Commissioner's office.

Although the OIPC is not recommending any changes to PIPA at this time, background information is being provided so the Committee can better understand this issue and the Commissioner's concerns.

Background

Solicitor-client privilege applies to communications between a lawyer and a client, where legal advice is sought or given and is intended to be confidential. The purpose of solicitor-client privilege is to promote full and open communications between a lawyer and his or her own client. Generally, information that is protected by solicitor-client privilege is not admissible as evidence in proceedings and is not required to be disclosed.

PIPA and Solicitor-Client Privilege

Under PIPA, individuals have a general right of access to their own personal information, subject to exceptions and taking into account what is reasonable. For example, an organization may, but is not required to, refuse to provide access to personal information if "the information is protected by any legal privilege" (PIPA, section 24(2)(a)). This discretionary exception to disclosure under section 24(1)(a) includes information protected by solicitor-client privilege. If an organization applies an exception to disclosure, such as solicitor-client privilege, to the personal information being requested, the individual requesting access can ask the Commissioner to review whether the organization properly applied the exception.

The power of the Commissioner to review an organization's response to an access request is among the Commissioner's most important functions. PIPA is based on the concept that an individual has the right to control his or her own personal information, and the access rights enshrined in PIPA allow individuals to exercise this right of control. Access allows an individual to know what personal information an organization has about them. When an organization applies an exception, the Commissioner must have the ability to review the records being withheld from an individual.

Under PIPA, an individual is entitled to access only his or her personal information. In many cases, the information in a lawyer's file is not about an individual and is therefore not personal information and not subject to an access request. Commissioner's orders have confirmed this. There is no reason for an organization to rely on solicitor-client privilege to withhold information that an individual has no right to access to begin with.

In those cases where records are subject to an access request, experience has shown that organizations' claims of solicitor-client privilege are not always correct. In many cases, the Commissioner can make a determination as to whether the exception applies based on evidence from the organization about the record, but sometimes it is necessary for the Commissioner to review the record itself to determine whether an exception has been properly claimed.

The Commissioner's power to review records is set out in section 38(2) of PIPA under which "the Commissioner may require any record to be produced" and "may examine any information in a record". Section 38(3) of PIPA requires an

organization to produce a requested record to the Commissioner, "notwithstanding any other enactment or any privilege of the law of evidence". This phrase: "any privilege of the law of evidence" is used in many other access and privacy statutes in Canada.[32]

Until recently, courts across Canada had consistently held that "any privilege of the law of evidence" included solicitor-client privilege.[33] The Alberta Court of Appeal, however, in *University of Calgary v. JR*,[34] held that "any privilege of the law of evidence" did not include solicitor-client privilege. The Supreme Court of Canada granted the Commissioner leave to appeal the decision, and the case is currently scheduled to be heard on April 1, 2016.

As a result of the Court of Appeal's decision, there is a growing trend before the Commissioner's office where organizations withhold records at issue in an access request on the ground that they are solicitor-client privileged. The organizations then refuse to provide any further information about the records and refuse to let the Commissioner review the records to determine whether the exception has been properly applied. Accordingly, other than an organization's own assertion, there is no way to determine whether the exception has been properly applied. This has led to a growing number of cases where the Commissioner must issue a formal Notice to Produce the records at issue to an organization, and a growing number of cases ending up before the courts as organizations seek judicial review of the Notices to Produce.

Where it is necessary to review a record, the Commissioner will review it *only* to determine whether the privilege has been properly claimed; the Commissioner is not an interested party in the content of the records, other than to ensure that they are subject to the exception claimed. These records are not made public or put to any other purpose other than ensuring the privilege was properly claimed. Further, the Commissioner

---

32 **Alberta**: *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25, s. 56(3), and *Health Information Act*, RSA 2000 c H-5, s. 88(3).

Federal (Canada): *Access to Information Act*, RSC 1985, c. A-1, s. 36(2), and *Privacy Act*, RSC 1985, c. P-21, s. 34(2) Both Acts refer to "any privilege under the law of evidence".

British Columbia: *Freedom of Information and Protection of Privacy Act*, RSBC 1996 c. 165, s. 44(3), and *Personal Information Protection Act*, SBC 2003, c. 63, s. 38(5), which refers to "any privilege afforded by the law of evidence"

Manitoba: *Personal Health Information Protection Act*, CCSM c. P33.5, s. 29(5), and *The Freedom of Information and Protection of Privacy Act*, CCSM c F175 s. 50(3).

Ontario: *Freedom of Information and Protection of Privacy Act*. 52(1), and *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c. M.56, s. 41(4). Both Acts state: "despite Parts II and III of this Act or any other Act or privilege".

New Brunswick: *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, s. 62, and *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6, s. 62.

33 *District No. 49 (Central Coast) v. British Columbia (Information and Privacy Commissioner),* 2012 BCSC 427 at paras 49-50 and 55; *Newfoundland Labrador (Information and Privacy Commissioner) v. Newfoundland and Labrador (Attorney General),* 2011 NLCA 69 at paras. 37 and 52; *University of Calgary v. JR,* 2013 ABQB 652 at paras. 226 – 229 (overturned at CA, infra; leave to appeal to SCC granted).

34 *University of Calgary v. JR,* 2015 ABCA 118.

does not request the production of records over which privilege has been claimed in every case; in fact, the Commissioner has developed a detailed *Solicitor-Client Privilege Adjudication Protocol*, which sets out numerous steps regarding information to be provided regarding a claim of privilege before the organization will be required to produce the actual records. The Commissioner will require production of the actual records only as a last resort if all other steps have failed.

If the Commissioner finds that a record over which a claim of privilege has been asserted is not actually privileged, the Commissioner does not disclose it. The Commissioner must return all records to the organization after they have been reviewed (PIPA, section 38(5)). Where an exception does not apply to a record, the Commissioner will order the organization to disclose the record to the Applicant, and this order is subject to judicial review if the organization disputes the Commissioner's decision.

In the 2006-07 review of PIPA, the Special Select Committee "appreciated that, without the ability to examine the records, the Commissioner cannot provide a complete review of an organization's response to an access request."[35] Two changes were made to the legislation to create certainty for organizations concerning the protection of solicitor-client privilege when privileged records are provided to the Commissioner:

- Section 38.1 of PIPA was added to confirm that legal privilege would not be affected by disclosing the information to the Commissioner; and
- Section 41(3.2) was added to confirm that the Commissioner shall not disclose information subject to solicitor-client privilege to the Minister of Justice or Solicitor General.

At this time, the OIPC is not recommending any additional changes to PIPA. The OIPC is of the opinion that the current wording of the legislation "notwithstanding any privilege of the law of evidence" is sufficiently clear, and that it includes solicitor-client privilege. Further, this exact issue will be heard by the Supreme Court of Canada in April 2016. In the event that the Supreme Court of Canada provides guidance that affects the current interpretation of PIPA, the Commissioner will notify the Committee (or appropriate party) at that time.

35 Special Select *Personal Information Protection Act* Review Committee, Final Report, November 2007, page 35.

Commissioner's Standing Before the Courts

"Standing" refers to the right of the Commissioner to appear before a court when one of the Commissioner's decisions is being judicially reviewed.

PIPA requires the Commissioner to issue an order upon completing an inquiry. An order may, for example, direct an organization to provide, or not to provide, an individual with access to his or her own personal information, or to stop collecting, using or disclosing personal information in contravention of PIPA.

An order issued by the Commissioner is binding on the parties and is final (section 53). There is no right of appeal to the court; however, an individual or organization can apply to the Court of Queen's Bench for a judicial review of a Commissioner's order (section 54.1). Judicial review means that the Commissioner is subject to the law – a party may apply for a judicial review if they believe the Commissioner has made an unreasonable or incorrect decision, exceeded the Commissioner's jurisdiction, or has exercised the Commissioner's power in an arbitrary, unreasonable or discriminatory way.

A Court of Queen's Bench decision with respect to a judicial review is then subject to appeals to higher courts.

Currently, the Commissioner has no automatic right to appear before the Court of Queen's Bench or a higher court as a full or "true" party; rather, the Commissioner's standing must be determined by the court in each case. This uncertainty in every case before the courts is problematic because only the Commissioner has the ability to inform the court of the public interest and policy positions supporting the Commissioner's decisions. Further, the Commissioner is usually in the best position to help the court understand the complexities of the legislation at issue. Often these complexities may not be understood by the party challenging the Commissioner's decision, or may not be put forward to the court. In most cases the individual whose complaint or request for review is the subject of judicial review does not even appear before the court, so if the Commissioner does not appear, the court will hear only from the party disputing the decision at issue.

In some cases, it is necessary for the Commissioner to appeal a court's judicial review decision because the decision, while it may have focused on the limited issues between the parties, has a broader effect of undermining the public interest or a fundamental principle underlying PIPA.

Court Cases Regarding Standing

The Commissioner faces uncertainty in every court case as to whether the Commissioner will be allowed to participate, and if so, the extent of participation before the court.

The Alberta Court of Appeal recognized the Commissioner as being "very close to a true party" in *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*[36] (*Leon's*). Importantly, in that case the Commissioner did not bring the appeal, but was responding to

36 *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*, 2011 ABCA 95.

another party's appeal of a lower court decision. The Court of Appeal stated, "The Commissioner is very close to being a true party. It is unrealistic to think that the original complainant would have the resources or the motivation to resist the application for judicial review. If the Commissioner does not resist the judicial review application, no one will."[37]

However, more recently, that same court refused the Commissioner standing to appeal a decision. In *Imperial Oil v. Alberta (Information and Privacy Commissioner)*,[38] (*Imperial Oil*) the Alberta Court of Appeal refused to allow the Commissioner to initiate an appeal. The unfortunate result was that despite the very serious concerns the Commissioner had regarding the broader policy implications of the lower court's decision, the Commissioner had no standing to appeal those matters. Although the Imperial Oil case was decided under FOIP, not PIPA, it will likely act as a precedent in which the Commissioner is also prevented from appealing judicial review decisions under PIPA.

Currently, the Alberta Court of Appeal may grant the Commissioner standing as a party when another party brings an appeal (*Leon's*), but will not allow the Commissioner to bring an appeal (*Imperial Oil*). The situation is different again before the Supreme Court of Canada, where the Commissioner has been recognized as a full party in three cases, both where another party brought the appeal and where the Commissioner initiated the appeal.

A recent case from the Supreme Court of Canada reviewed the law on standing of administrative tribunals (see: *Ontario (Energy Board) v. Ontario Power Generation Inc.*, 2015 SCC 44). In this case, the Board had a limited statutory right of appeal in its enabling legislation (*Ontario Energy Board Act*, 1998, c15, Sch. B, section 33(3)). Another Ontario statute (*Judicial Review Procedure Act*, RSO 1990, c.J-1, section 9(2)), provides administrative tribunals, including the Information and Privacy Commissioner of Ontario, with standing before a court as a party on judicial review; however, the statute does not address the scope of participation; therefore, the scope remains in the Court's discretion.

A PIPA amendment addressing the Commissioner's standing before the courts should also address the scope of the Commissioner's participation. The Commissioner submits that PIPA include a provision that specifies the Commissioner has standing as a full party to appear and make submissions as a full party on judicial reviews of the Commissioner's decisions, and to initiate and appear on appeals from judicial review decisions on the same basis.

The proposed provision will bring consistency to the current uncertainty regarding the Commissioner's standing before the courts. It will ensure that the Commissioner's voice will be heard by the courts, and will allow the Commissioner to explain the public interest and the policies that the Commissioner is statutorily mandated to forward. It will also recognize the

37 Ibid at para 30.

38 *Imperial Oil v. Alberta (Information and Privacy Commissioner)*, 2014 ABCA 276.

Commissioner's important function as an Officer of the Legislature: the Commissioner does not just adjudicate disputes between parties; the Commissioner also makes policy, educates, initiates and investigates complaints (or can decline to investigate a complaint), and conducts a number of other functions. Unlike many tribunals, the Commissioner's adjudicative function is aimed towards building public policy, rather than resolving private disputes.

Recommendation

8. **That PIPA be amended to provide that the Commissioner has standing as a full party to appear and to make submissions as a full party on judicial reviews of the Commissioner's decisions, and to initiate and appear on appeals from judicial review decisions on the same basis.**

Costs

In Canada, regardless of the outcome of a judicial review, a tribunal rarely pays or is paid costs (see: *Brewer v. Fraser Milner Casgrain*, 2008 ABCA 160 at paragraph 23).

The Commissioner is not adverse to any other party in a judicial review proceeding. The Commissioner's primary role on judicial review is to assist the court in understanding the decision being reviewed, and in particular, the underlying policy and public interest on which the decision is based. As such, consistent with Canadian common law, the Commissioner should neither be awarded costs nor be subject to paying them. A provision in PIPA which formally recognizes the Commissioner as a party to judicial review proceedings, should not affect this general legal principle; however, enshrining this principle in a statutory amendment will resolve any uncertainty and will remain consistent with Alberta and Canadian law. Similar provisions are found in other tribunal statutes, such as the aforementioned *Ontario Energy Board Act* (section 33(5)).

The OIPC further recommends that in addition to the above statutory amendment granting the Commissioner standing before the courts, a further amendment should provide that the Commissioner is not subject to paying or receiving costs awards in respect of participation in a judicial review proceeding.

Recommendation

9. **That PIPA be amended to provide that the Commissioner is not subject to paying or receiving costs awards in respect of participation in a judicial review proceeding.**

Commissioner's Orders

After conducting an inquiry, the Commissioner is required to dispose of the issues by making an order (section 52(1)).

Section 52(2) lists the orders the Commissioner may make when the inquiry relates to the organization's decision on whether to give an individual *access* to his or her personal information or to provide information about the use or disclosure of his or her personal information. Section 52(2) was amended after the previous PIPA review to allow the Commissioner to make an order that the Commissioner considers appropriate when none of the listed orders would be applicable in the circumstances of a particular case(section 52(2)(b)).

Section 52(3) sets out the orders the Commissioner can make when the inquiry relates to a matter *other than an access request* referred to in section 52(2). However, there are instances where none of the enumerated orders in section 52(3) are applicable under the circumstances. For example, section 52(3)(a) allows the Commissioner to confirm that a duty owed under PIPA has been performed by the organization or to require the organization to perform the duty, but the inquiry might determine that there was no duty owed by the organization under the Act. In other situations, an issue might be moot so that there is no reason to make one of the specified orders.

A technical amendment to section 52(3) is therefore proposed – that section 52(3) be amended to include a provision similar to section 52(2)(b) to allow the Commissioner to make an order that the Commissioner considers appropriate when none of the orders currently listed in section 52(3) would be applicable.

Recommendation

10. That section 52(3) of PIPA be amended to allow the Commissioner to make an order that the Commissioner considers appropriate if, in the circumstances, an order currently listed in section 52(3) would not be applicable.

Summary of Recommendations

1. That PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year transition period.

2. That PIPA be amended to require that organizations have a privacy management program in place and that organizations provide information about their privacy management programs to the Commissioner and to individuals, upon request.

3. That no changes be made to the Act's disclosure without consent provisions pertaining to disclosures without a warrant.

4. That PIPA be amended to address publication of transparency reports. Amendments should consider:

    - whether the reports should be limited to disclosures upon request of law enforcement or government agencies, or include disclosures made pursuant to legislation or on a voluntary basis;
    - the intervals for reporting; and
    - the minimum elements to be reported, such as the number and nature of the requests or disclosures, the legal authority for the request or disclosure, the response to requests (e.g. fulfilled, rejected, challenged), and the number of individuals or accounts involved.

5. At this time, the OIPC is not recommending any additional changes to PIPA concerning freedom of expression. However, should the committee identify any organizations as needing a special provision for their expressive rights then the OIPC recommends those organizations should be included within the scope of a provision that provides for the balancing of the purposes of the expression with the privacy interests of individuals.

6. That PIPA be amended to require organizations having personal information in their custody to notify the organization having control of the same personal information, without unreasonable delay, of any incident involving the loss of or unauthorized access to or disclosure of personal information.

7. That the *PIPA Regulation* be amended to require organizations to provide information to the Commissioner about the relationship with a service provider when a service provider is involved in a breach incident.

8. That PIPA be amended to provide that the Commissioner has standing as a full party to appear and to make submissions as a full party on judicial reviews of the Commissioner's decisions, and to initiate and appear on appeals from judicial review decisions on the same basis.

9. That PIPA be amended to provide that the Commissioner is not subject to paying or receiving costs awards in respect of participation in a judicial review proceeding.

10. That section 52(3) of PIPA be amended to allow the Commissioner to make an order that the Commissioner considers appropriate if, in the circumstances, an order currently listed in section 52(3) would not be applicable.

Appendix F: ***Producing Records to the Commissioner: Restoring Independent and Effective Oversight under the FOIP Act*** **(April 2017)**

Producing Records to the Commissioner

Restoring Independent and Effective Oversight under the FOIP Act

April 2017

A Special Report and Request for Legislative Amendment
Submitted to the Legislative Assembly of Alberta

Office of the Information and
Privacy Commissioner of Alberta

Introduction

Two recent developments have compromised the operation of the *Freedom of Information and Protection of Privacy Act* (FOIP Act) and my ability to perform my functions as an Officer of the Legislature under that statute.

First, the Supreme Court of Canada in *Alberta (Information and Privacy Commissioner) v. University of Calgary* [1] (U of C case) said that the Legislature did not use the right words in the FOIP Act[2] to allow me to require public bodies to give me records over which public bodies are claiming solicitor-client privilege. Those records are often very important evidence in matters that I have to decide. This includes when I conduct independent reviews of decisions that records are subject to solicitor-client privilege and do not have to be disclosed to a citizen who requests access, and when I investigate public bodies to ensure they comply with their obligations under the FOIP Act.

Second, public bodies have not been giving me those records when I need them as evidence for decisions I must make. During the time that the U of C case was making its way through the court system, many public bodies, especially government, were refusing to provide me with records over which solicitor-client privilege and other similar privileges were being claimed. This happened despite a 2008 letter from the then-Minister of Justice and Attorney General to the former Commissioner, saying that, "You currently have the power to compel production of all records subject to review, even where such records are subject to privilege."[3] In addition, the Court of Queen's Bench had said that as Commissioner, I had the power to require that those records be provided to me for my review.[4]

After the Supreme Court of Canada issued its decision in November 2016, I issued a public statement in which I said that I would be writing to government with options for proceeding on this matter.[5] However, as an independent Officer of the Legislature who reports to the

1 *Alberta (Information and Privacy Commissioner) v. University of Calgary*, [2016] 2 SCR 555, 2016 SCC 53 (CanLII), http://canlii.ca/t/gvskr.
2 Related to "Powers of Commissioner in conducting investigations or inquiries", Section 56(3) of the FOIP Act reads that the Commissioner may require any record "despite any other enactment or any privilege of the law of evidence".
3 A copy of this letter is attached as Appendix 1.
4 *University of Calgary v JR*, 2013 ABQB 652 (CanLII), http://canlii.ca/t/g1t5g.
5 "Commissioner Issues Statement in Response to Supreme Court of Canada Decision", Office of the Information and Privacy Commissioner, November 25, 2016, retrieved from https://www.oipc.ab.ca/news-and-events/news-releases/2016/commissioner-issues-statement-in-response-to-supreme-court-of-canada-decision.aspx.

Legislative Assembly and not to government, and whose ability to perform core functions as an Officer of the Legislature has been compromised, I have decided instead to submit this special report to the body to which I report.

The Legislature established the position of Information and Privacy Commissioner to provide for an accessible, affordable and timely process for reviewing access to information decisions made by public bodies. The Legislature now has an opportunity to clearly state its intentions about how decisions involving solicitor-client privilege, and other similar privileges, are to be made.[6] If the Legislature decides that its own Officer is to have that power (as was previously assumed to be the case), then this is the Legislature's opportunity to amend the FOIP Act and "get the words right". I am requesting that the FOIP Act be amended to explicitly state that I have the power to require public bodies to produce to me records over which solicitor-client privilege and other similar privileges are claimed, when in my opinion it is necessary to review those records (such as when a public body does not provide enough evidence to satisfy me that the records are privileged).

The Legislature established the position of Information and Privcy Commissioner to provide for an accessible, affordable and timely process for reviewing access to information decisions made by public bodies.

This report provides background information for this important issue and my request for amendment, as well as a brief explanation of access to information and the role my office plays.

The Importance of Access to Information

Access to information enhances citizens' trust in government.

Transparency in the functioning of government permits citizens to participate in their democracy and promotes government accountability. For this reason, the right of access has been deemed quasi-constitutional by the Supreme Court of Canada.[7]

6 Other privileges that may give rise to similar contention are litigation privilege and informer privilege.
7 *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 SCR 773, 2002 SCC 53 (CanLII), http://canlii.ca/t/51qz.

In Dagg v. Canada (Minister of Finance), La Forest said:[8]

> The overarching purpose of access to information legislation is to facilitate democracy by helping to ensure that citizens have the information to participate meaningfully in the democratic process and that politicians and bureaucrats remain accountable to the citizenry.

As Rowat explains in a classic article:[9]

> Parliament and the public cannot hope to call the Government to account without an adequate knowledge of what is going on; nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view.

A formal right to access information is not useful for these purposes if it is not accessible to citizens. As well, access to information often is not valuable or meaningful unless it is timely. If it takes months or even years to obtain information, the information may not be useful once it is received.

Access to Information in Alberta

Since 1995, Alberta citizens – including individuals, community and advocacy groups, businesses, media, and elected officials – have had the right to ask government and other public bodies for information about public bodies' programs and activities. Individuals may also ask for their own personal information.

The FOIP Act provides this right of access to citizens and sets out specific exceptions under which records do not have to be disclosed in response to a request for access.

Citizens request access to information from public bodies. If a citizen is dissatisfied with a public body's decision, they have a right to ask my office to review that decision. My office was established to be more accessible, affordable and timely for citizens than using the courts to make these decisions.

Since 1995, Alberta citizens including individuals, community and advocacy groups, businesses, media, and elected officials have had the right to ask government and other public bodies for information about public bodies' programs and activities.

8 *Dagg v. Canada (Minister of Finance)*, [1997] 2 SCR 403, 1997 CanLII 358 (SCC), http://canlii.ca/t/1fr0r, para. 61.
9 Professor Donald C. Rowat *How Much Administrative Secrecy?* (1965), 31 Can. J. of Econ. and Pol. Sci. 479, at p. 480.

When a citizen asks for a review of a public body's access decision, there is usually an initial phase in which the matter is informally mediated by my office to see if a resolution can be achieved. If the matter is not resolved, the citizen can request a formal inquiry. If the matter goes to inquiry, I or my delegated Adjudicators may issue an order that is binding on the public body and is enforceable in the Court.

When my office conducts a review of an access decision, the records are important and valuable evidence for determining whether they do or do not meet the criteria of an exception. For this reason, when the Legislature enacted the FOIP Act, it gave me the power to look at all records that are requested, and to require the records be given to me when not provided voluntarily.

One of the exceptions to disclosing records to a citizen who has asked for them is when the records are subject to "solicitor-client privilege". Public bodies often claim this exception.[10] If, after a review by my office, the claim for solicitor-client privilege is upheld, the records are not disclosed.

The FOIP Act's wording is that I have the power to decide whether records meet the criteria for privilege as an exception to disclosure, and that I have the power to require the records to be provided to me "despite any privilege of the law of evidence".[11]

For nearly 18 years, public bodies accepted that the Legislature intended... that my predecessors and I could review records over which solicitor-client privilege was being claimed...

For nearly 18 years, public bodies accepted that the Legislature intended by this that my predecessors and I could review records over which solicitor-client privilege was being claimed, and they routinely gave my office such records to help me to decide whether to either confirm or deny a claim of solicitor-client privilege. As already noted, in 2008, the then-Minister of Justice and Attorney General wrote to the former Commissioner, saying that, "You currently have the power to compel production of all records subject to review, even where such records are subject to privilege."[12]

10 There are approximately 80-90 files in the office that involve claims that this privilege applies.
11 This provision is contained in section 56(3) of the FOIP Act.
12 A copy of this letter is attached as Appendix 1.

Despite the common understanding that I had this power, my office does not routinely require production of records alleged to be subject to solicitor-client privilege. Since 2008, my office has had in place a process for dealing specifically with records over which solicitor-client privilege has been claimed, to ensure that my office is not requiring those records to be produced unless it is necessary to review those records to decide whether they are privileged. The current process allows public bodies to instead provide an affidavit and includes a schedule in which the public body lists the records for which the privilege is claimed, along with the description for each record. The test to be met for each claim of privilege is set out. The description for each record must be sufficient to meet that test, without revealing the privileged information. In many cases, this is sufficient evidence for the purposes of my decisions.

The power to review records as evidence for investigations is also important when performing my responsibilities of ensuring that public bodies have put in place appropriate measures for dealing with access requests and protecting privacy. My recent Investigation Report F2017-IR-03 of the government into the issue of delays and possible political interference in the access request response process has been thwarted by the refusal of the former and current governments to give me access to records.[13]

Alberta (Information and Privacy Commissioner) v. University of Calgary

Despite the longstanding assumption by my office and public bodies that I may require records over which solicitor-client privilege is claimed, in November 2016, the Supreme Court of Canada decided that the Legislature had not used the right language in the FOIP Act to show that it intended to give the Commissioner the power to require those records. The Court said that I did not have the power, but it did not say how I was to decide the issue when I do not have sufficient evidence in the absence of the records.

The Court's decision was based largely on the idea that solicitor-client privilege is not just a rule of evidence, and has evolved into a substantive rule. The substantive rule contemplates that legislative provisions can override solicitor-client privilege, but the words used must be clear. The Court said that the words "solicitor-client privilege" do not necessarily need to be used, but that the words "despite any privilege of the law of evidence" were not clear enough.

13 This investigation report is available at www.oipc.ab.ca.

In the result, unless more specific language is put in place, either I will have to decide whether records are subject to solicitor-client privilege in the absence of conclusive evidence (which is untenable), or decisions about solicitor-client privilege will have to be transferred to the courts.

Request for Legislative Amendment

I am requesting that the Legislature amend the FOIP Act to state:

- That I have the power to require public bodies to produce to me records over which solicitor-client privilege and other similar privileges (e.g., litigation privilege, informer privilege) are claimed.
- That I may require those records when, in my opinion, it is necessary to perform my functions (such as when a public body does not provide enough evidence to satisfy me that the records are privileged).
- That solicitor-client privilege or other legal privilege is not waived when the privileged records are provided to me.
- That I may not disclose to the Minister of Justice and Solicitor General, as evidence of an offence, records to which solicitor-client privilege applies.[14]

The amendments I request will enable me to continue to achieve a fundamental purpose of the FOIP Act: to ensure citizens who wish to participate in the democratic process and hold their government to account have the means to obtain information from public bodies in an accessible, affordable and timely way.

The alternative is to transfer the power of the Commissioner under the FOIP Act to the courts, and have the courts decide whether a public body properly applied solicitor-client privilege to records when responding to an access request.

...to ensure citizens who wish to participate in the democratic process and hold their government to account have the means to obtain information from public bodies in an accessible, affordable and timely way.

14 The third and fourth requested amendments are already contained in the *Personal Information Protection Act*, which applies to private sector organizations in Alberta, in section 38.1 and section 41(3.2), respectively.

In my view, this approach is not feasible in light of the following disadvantages:

- It requires the Court to decide the issue when the Alberta Court of Appeal has already stated that, "Further, in this day of increasingly scarce judicial resources, judges should not be bogged down regularly by the need to examine volumes of records to assess privilege".[15]

- It requires increased resources of the Court at a time when those resources are stretched to the limit.[16]

- It requires that the Court have an expedited process to avoid lengthy delays (i.e., it currently takes a year to get before the Court on judicial reviews of my decisions).

- It increases the cost for public bodies, my office and citizens, and it will increase the number of unrepresented litigants before the Court.

- It entails multiple decision makers in a single case, as well as multiple appeal routes, unduly complicating and protracting the process.

- It permits the Court to decide an issue that it may not have constitutional jurisdiction to decide, such as when I require records to perform my function as an Officer of the Legislature in holding the government to account, and the government will not provide those records. This could be seen as a "dispute between the legislative and executive branches" of government, which is unenforceable by the Court.[17]

- It requires judges of the Court appointed as Adjudicators under section 75 of the FOIP Act to follow this same procedure, as Adjudicators appointed under section 75 have only those powers that I have under the FOIP Act.

---

15 *Canadian Natural Resources Limited v ShawCor Ltd.*, 2014 ABCA 289 (CanLII), para. 65, http://canlii.ca/t/g90h9.
16 (1) "Alberta to invest $14.5-million to ease court delays", The Globe and Mail, March 9, 2017, retrieved from www.theglobeandmail.com/news/politics/alberta-to-invest-145-million-to-ease-court-delays/article34262631/. (2) "Courts shaken by search for solutions to delays: A heretical idea is gaining traction as lawmakers seek to overhaul an unwieldy system: Maybe the justice system cannot do everything. Maybe it cannot prosecute every crime, Sean Fine reports", The Globe and Mail, March 12, 2017, retrieved from www.theglobeandmail.com/news/national/courts-shaken-by-search-for-solutions-todelays/article34275019/. (3) "Lengthy court delays reach 'crisis' level, justices and lawyers open 2017 calendars", Calgary Herald, October 27, 2015, retrieved from http://calgaryherald.com/news/local-news/lengthy-court-delays-reach-crisis-level-justices-and-lawyers-open-2017-calendars.
17 *Canada (Auditor General) v. Canada (Minister of Energy, Mines and Resources)*, [1989] 2 SCR 49, 1989 CanLII 73 (SCC), http://canlii.ca/t/1ft4w.

I previously laid out some of these disadvantages to government in my March 13, 2015 letter to the then-Minister of Justice and Solicitor General, concerning my office's investigation of possible political interference in the access request response process. In that letter, I said:

> The involvement of the Courts at the front end of my Office's processes, rather than at the back end [through judicial review], will have a significant impact on my ability to perform my legislated functions as the independent oversight body for the FOIP Act, in the following ways:
>
> - it will add considerable time to the length of investigations and reviews, thereby delaying access to information and resolution of complaints;
> - the process will be significantly more formal, requiring legal representation for all parties and deterring many applicants and complainants;
> - the costs for applicants/complainants, public bodies and my office will increase dramatically;
> - the already-burdened Courts will be required to accommodate an increased workload of cases that were formerly handled solely by my office as a quasi-judicial tribunal, resulting in further delays.

In summary, I respectfully request that the FOIP Act be amended to explicitly state that I have the power to require public bodies to produce to me records over which solicitor-client privilege and other similar privileges are claimed, when in my opinion it is necessary to review those records (such as when a public body does not provide enough evidence to satisfy me that the records are privileged).

Jill Clayton
Information and Privacy Commissioner of Alberta

Appendix 1: Letter from the former Minister of Justice and Attorney General

3500 12

ALBERTA
JUSTICE AND ATTORNEY GENERAL
Office of the Minister

RECEIVED
NOV 2 6 2008
INFORMATION & PRIVACY COMMISSIONER

AR 30981

NOV 2 5 2008

Mr. Frank Work, Q.C.
Information and Privacy Commissioner
#410, 9925 – 109 Street NW
Edmonton, AB T5K 2J8

Dear Mr. Work:

Thank you for your letter dated October 28, 2008 regarding the Solicitor-Client Privilege Adjudication Protocol you have recently adopted.

Solicitor-client privilege is a fundamental part of our legal system and ought to be protected wherever possible. I wonder however whether your protocol is unnecessarily complex.

You currently have the power to compel production of all records subject to review, even where such records are subject to privilege. The wording used in our various privacy statutes closely resembles what is present in the federal *Privacy Act*. While the Supreme Court unfortunately declined to consider the true effect of such wording, it is noteworthy that they did recognize that the intent is to enable the production of privileged records. As a result, you have such a power until a Court determines otherwise.

In the interim, the *Blood Tribe* decision offers some important comments on when such a power, if it is present, ought to be exercised. The suggestion is that the power to compel the production of privileged records should only be exercised judiciously and not as a rule. To that extent, your protocol for not demanding routine production of records over which solicitor-client privilege has been claimed is prudent.

I wonder whether the three options you provided under the protocol are not unnecessarily complicated. The decision in the *Blood Tribe* case would seem to suggest that the second option is the appropriate one. An attempt should be made to resolve the issue of privilege through evidence and argument first and that production of such records for your review should only be done as a last resort. I appreciate your attempt to answer all possible situations that may arise in this regard, however am concerned that in doing so the protocol has been rendered unnecessarily complex.

Thank you for the opportunity to provide you with my comments.

Yours truly,

Alison Redford, Q.C.
Minister

403 Legislature Building 10800 - 97 Avenue, Edmonton, Alberta Canada T5K 2B6 Telephone (780) 427 2339 Fax (780) 422 6621