Office of the Information and Privacy Commissioner of Alberta

DELIVERED BY EMAIL

November 20, 2024

Honourable Nate Glubish
Minister of Technology and Innovation
ti.minister@gov.ab.ca

Dear Minister Glubish,

RE: Commissioner's comments and recommendations regarding Bill 33 – *Protection of Privacy Act*

I am responding to the November 6, 2024 introduction of Bill 33 *Protection of Privacy Act* (Bill 33, PPA or the Act). The *Freedom of Information and Protection of Privacy Act* (FOIP Act) provides me with the ability to comment on the access and privacy implications of proposed legislative schemes.

As stated in my September 23 letter to the Ministry of Technology and Innovation on proposed amendments to the FOIP Act, I cannot overstate the importance of ensuring that adequate changes are made to Alberta's public sector privacy law to protect Albertans' privacy rights, allow for government program ambitions in a responsible way, and ensure uses of innovative technology are lawful, proportionate, and balanced by privacy controls and rights.

Having reviewed Bill 33, I believe the PPA could be strengthened to better protect the privacy rights of Albertans as Government advances the use of technology in the delivery of public services and for innovation purposes in the province generally. It is with this goal in mind that I made my comments and recommendations, which are attached to this letter.

I look forward to continuing to work with you and your team on improvements to this fundamentally important legislation and on the development of the regulations.

Sincerely,

Original signed by

Diane McLeod
Information and Privacy Commissioner

Office of the Information and
Privacy Commissioner of Alberta

Bill 33 Protection of Privacy Act

Comments and Recommendations from the Commissioner

November 20, 2024

Explanatory note

All sectional references in the following text are to Bill 33, *Protection of Privacy Act* (the Act or PPA), unless stated otherwise. "Sept 23/24 Letter" refers to the letter with comments on changes to the *Freedom of Information and Protection of Privacy Act* (FOIP Act) provided by the Office of the Information and Privacy Commissioner (OIPC) to the Ministry of Technology and Innovation (Ministry) on September 23, 2024. Any reference to "Previous Report" herein refers to the March 4, 2024 report, entitled *Freedom of Information and Protection of Privacy Act Comments and Recommendations from the Commissioner*, provided to the Ministry on that date.

Positive changes to the legislation

I am pleased to see the following included in PPA.

1. The requirement for public bodies to implement privacy management programs (PMPs) and conduct privacy impact assessments (PIAs) generally.
2. The requirement to report breaches generally.
3. The 'Data Part', i.e. the provisions that enable the ability to create and use new types of data, although regulation to do so responsibly will need to follow. I am pleased to see that non-identifying data will remain subject to the Act.
4. The notice requirement under PPA section 5(2)(d) regarding automated decision-making, although the content and method of such notice must be further detailed in the Act or regulation.
5. The prohibition on the sale of personal information in PPA section 11.
6. The substantial fines for offences committed under PPA.

Comments and recommendations for strengthening the Act

Paramountcy

Section 5 of the FOIP Act contains a paramountcy clause which applies to all Parts of that Act including Part 2 Protection of Privacy. This provision clarifies that if there is a conflict between the FOIP Act and any other Act, the provisions of the FOIP Act will prevail unless the other Act expressly states that it is paramount over the FOIP Act. PPA does not contain a paramountcy clause. We sought clarification from the Ministry about why this provision was not included in PPA. Their response was as follows.

> *"Technology and Innovation determined that an express paramountcy provision in Bill 33: Protection of Privacy Act was not required. Under the FOIP Act, the collection and disclosure of personal information is permitted if authorized by another enactment (see FOIP ss. 33(a), and 40(1)(e) and (f)), which mitigates any conflict between FOIP and another Act. The same provisions have been included in the proposed*

Protection of Privacy Act and it was determined that an express paramountcy provision was no longer necessary as there should not ever be a conflict between the proposed Act and another Act."

It may be that where another statute permits collection, use or disclosure of personal information, the section referred to by the Ministry in PPA that permits a public body to collect personal information that "is expressly authorized by an enactment of Alberta or Canada" (section 4(a) of PPA) could mean that PPA and the other statute could operate harmoniously in some circumstances. However, in the event the other statute permits collection, use or disclosure regardless of whether this is necessary to carry out its purposes (as limited by sections 12(4) and 13(4) of PPA), there may still be a conflict. For example, the *Security Services and Investigators (Ministerial) Regulation, Alta Reg 55/2010*, requires an applicant to provide "e) a criminal record check, a police information check and vulnerable sector search" all of which may contain more information than is reasonable for the purpose for which the information is collected. As well, PPA creates the right to have information collected directly unless indirect collection is authorized by the other statute or by another provision of section 5. It also prohibits uses other than those authorized under section 12. If the other legislation fails to address these issues in a manner consistent with PPA, there may be a conflict.

It is my view[1] that having a single statute governing dealings with personal information by public bodies is more practical. Any time another statute could equally govern dealings with information, it is necessary to review all possible statutes before deciding whether a given dealing with information is authorized other than by PPA. To analyze how the various statutory provisions relate to one another is an unduly complex process.

Without a paramountcy clause in PPA, subordinate legislation other than a statute or regulation (e.g. a bylaw) could be used to override the important protections for privacy, such as, for example, the prohibition on selling personal information enshrined in PPA. It is also possible that other Acts, regulations, or other subordinate legislation already exist, that are now appropriately limited by the privacy protections in the FOIP Act due to the paramountcy provision. Once PPA is enacted without a paramountcy provision, it cannot provide the same privacy protection as the FOIP Act did. It is unclear what the reason would be for eliminating the paramountcy provision even if it were redundant, which, for the reasons given, it is not.

Furthermore, the inclusion of a paramountcy clause in PPA recognizes the fundamental and quasi-constitutional nature of PPA as a law that is designed to protect privacy rights. This provision would ensure that where there may be a conflict between PPA and another law enacted for some other specific or particular purpose, the privacy rights as codified in PPA prevail to the extent of any conflict. Lastly, most privacy laws in Canada include a paramountcy clause. PPA would stand apart from these laws if enacted without one.

[1] For further reference see Commissioner's Orders on this point: F2007-001, F2007-002, H2011-001 at paras 50 and 51.

Recommendation:

1. It is recommended that a paramountcy provision be included in PPA.

Common or integrated program or service

PPA does define what a "common or integrated program or service" is. However, no controls have been added for the exercise of this authority to collect, use, or disclose personal information between public bodies. This is highly problematic in the digital age, where personal information can be integrated with ease among and within information systems, which in turn creates risks to Albertans if not properly mitigated with balanced rights and controls, including proper oversight.

The privacy and information landscape today is significantly different than it was decades ago when public bodies collected, used and disclosed personal information as part of a common or integrated program or service, largely within a paper-based public sector. For these reasons, in the Previous Report we set out in section 7.1 the need to include guardrails to the exercise of this authority in the digital age. We highlighted that modern privacy laws codify the requirements for a common or integrated program or service to be transparent about these programs or services and to increase accountability for reliance on this authority to collect, use or disclose personal information. Examples of these models are included in British Columbia's *Freedom of Information and Protection of Privacy Act* (BC FIPPA) and Yukon's *Access to Information and Protection of Privacy Act* (YK ATIPPA). Specifically, these Acts outline a process for establishing a common or integrated program or service, including agreements as well as a ministerial order (in the case of BC FIPPA) and approval by the Commissioner in Executive Council[2] (in the case of YK ATIPPA). Both require the submission to the Information and Privacy Commissioner of a PIA for review and comment, and the YK ATIPPA also requires publication of a report about such programs or activities, which supports transparency.

If this authority is to be relied on for data-driven activities, including for those set out in Part 3 of the Act[3], we strongly recommend that PPA incorporate a similar framework to BC FIPPA and YK ATIPPA to ensure privacy rights are respected.

The failure to establish controls in regard to the common or integrated program or service authority to collect, use or disclose personal information for data-driven initiatives as recommended, will, in my view, threaten the privacy rights of Albertans and risk the failure of these projects undertaken by government.

Additionally, I have concerns about the gaps in governance and accountability for personal information involved in a common or integrated program or service. As written, PPA does not establish which public body (among public bodies working together as part of a common or integrated program or service) is

[2] The Commissioner in Executive Council has a position similar to that of the Lieutenant Governor of Alberta.
[3] Part 3 Data Matching, Data Derived from Personal Information and Non-personal data.

responsible for accuracy and security requirements, correction and access requests, breach notification, or any other duties under the Act. As such, we recommend clarifying how accountability will be managed under the Act as it pertains to any personal information involved in a common or integrated program or service.

Recommendation

2. It is recommended:

    a. that guardrails like those that are included in BC FIPPA and YK ATIPPA be incorporated into PPA regarding the authority of public bodies to collect, use and disclose personal information for a common or integrated program or service; and

    b. that accountability for personal information involved in common or integrated program or service be incorporated into PPA including as it relates to the duties for accuracy and security requirements, correction and access requests, breach notification, and other duties under the Act.

Data matching

Data matching, section 17, involves the creation of data derived from personal information based on linking existing personal information (existing in two or more databases or other electronic sources of information). This process needs to be transparent to ensure the public is aware that new personal information about them is being generated. Transparency is particularly important when new personal information about an individual is generated without their knowledge. An individual's awareness of how their personal information is collected, used, or disclosed is essential to their ability to control it. Whenever personal information is collected without notice, it is necessary to compensate with transparency. Indeed, this transparency is essential to an individual's ability to exercise their rights under the Act, including the right of access.

Section 17(1)(a) permits a public body to carry out data matching to create data derived from personal information for research and analysis. It would be useful to clarify these terms to avoid overly broad interpretations. The ability to prescribe purposes for the exercise of section 17(1)(c) creates uncertainty about how this authority may be exercised by a public body. As such, it is recommended that the Commissioner be involved in the addition of any prescribed purposes permitted under this section.

Recommendation

3. It is recommended that:

    a. for any data matching that occurs under section 17, the public body that exercises this authority be required to publish information about the data matching, including the

data sources used, a description of the personal information created, and the purposes of the data matching;

b. the terms "research and analysis" in section 17(1)(a) be defined; and

c. for the addition of any prescribed purposes under section 17(1)(c), consultation in the form of review and comment by the Commissioner be required before any purposes are prescribed thereunder.

Purpose statement

Throughout PPA there are references to "personal privacy", a term which is not defined in the Act. Its meaning within PPA, where referenced, has no context. To remedy this issue, it is recommended that the section 2(c) purpose statement be modified to read *"to protect the personal privacy of individuals by controlling the collection, use, disclosure and protection of personal information by a public body or as otherwise permitted by this Act"*. Making this change would strengthen the protection of privacy overall within the Act as it would support interpretations that weigh in favour of protecting this right and align more closely with the title of the Act.

Recommendation

4. It is recommended that the purpose statement in section 2(c) be modified to "*to protect the personal privacy of individuals by controlling the collection, use, disclosure and protection of personal information by a public body or as otherwise permitted by this Act".*

Excluded personal information

Under sections 3(1)(s) and (t), in their role as ministers, members of the Executive Council may process or hold records that should be protected by PPA. Excluding these records, as these sections currently do, is contrary to the purposes of the Act and it is unclear what the policy rationale or public interest benefit would be from this change. Similarly, section 3(1)(t) removes the application of PPA from any record of communication between a political staffer and a Minister. These carve-outs from the application of PPA mean that a member of the Executive Council may collect, use, or disclose personal information for any purpose and communicate the same to a political staffer, and is not required to protect it. This is highly concerning, particularly given that a public body may disclose personal information under section 13(1)(g) to a member of the Executive Council if the information is necessary for a member's performance of a duty.

Recommendation

5. It is recommended that the carve-outs in sections 3(1)(s) and (t) be removed from PPA.

Security and breach provisions

Section 10 of PPA falls significantly short of security provisions required in comparable legislation.

- Section 10(1) does not adequately address minimum security requirements or efforts, or delegation to regulation of such minimum requirements[4], and should include a requirement to establish a security management program.
- Section 10 (2) misses the event of unauthorized alteration or modification of personal information.
- Section 10(3) should specify[5] breach notification content.

In addition, the breach notification requirements should include a provision for assessment of harm[6]; a requirement of the public body to provide a report to the Commissioner about the cause of the breach and the steps taken to mitigate the risks to individuals from the breach and to prevent recurrence; the power of the Commissioner to issue recommendations upon receiving a breach report; and a requirement for the public body to respond to the Commissioner's recommendations in writing about whether it accepts or rejects these recommendations. It is my view that these additional requirements should be included in the Act before it takes effect to ensure that breach notification, remedy, and prevention of recurrence is effective.

I am also of the view that breach reporting should be mandatory where there is a breach of the security requirements in section 20 for derived data from personal information and in section 24 for non-personal data.

Recommendation

6. It is recommended that section 10 be modified:
    a. to include minimum security requirements that a public body must maintain for any personal information in its custody or control;
    b. to include a requirement that public bodies establish and maintain a security management program;
    c. by adding unauthorized alteration or modification of personal information to the circumstances listed in section 10(2) that trigger the duty to notify about a breach, and

[4] See, e.g., HIA section 60, article 32 of GDPR, or section 30 of YK ATIPPA and YK Access to Information and Protection of Privacy Regulation, section 9.
[5] See, e.g., HIA section 60.1 and *Health Information Regulation* sections 8.1, 8.2, 8.3 or YK ATIPPA section 32.
[6] As is contained in section 60.1(4) of HIA.

add to this duty the requirement to report a breach of the security requirements in sections 20 and 24;

d. by specifying the content of a breach notification in section 10(3);

e. by adding an assessment of harm provision;

f. by adding the duty of a public body to provide a report to the Commissioner about the breach including how it occurred, what steps were taken to mitigate the risk of harm and the steps a public body will take to prevent recurrence;

g. by adding the authority of the Commissioner to review and comment on the report received and to make any recommendations necessary to mitigate the risks from the breach; and

h. to require the public body to provide its response in writing to the Commissioner regarding any recommendations made by the Commissioner, and whether it will accept or reject the recommendations.

Disclosure in the best interests of a minor

The authority to disclose personal information without consent under section 13(1)(ee) is very concerning. If disclosure is truly "in the best interests of a minor" then it should be with consent. It should be up to a minor who has capacity to decide for themselves about whether a disclosure of their personal information is in their best interests. The same can be said for the disclosure of personal information about the minor's parent or guardian. At the very least, added to the end of section 13(1)(ee) should be "and obtaining the consent of the minor or their parent or guardian, as applicable, is unattainable or impracticable and disclosure is not against any expressed wish of the individual whose personal information is disclosed under this section".

It is unclear in this section who is responsible for making the determination that disclosure is in the best interests of the minor and what "best interests" means. It is clearly less than harm or danger because if this were the case, section 13(1)(cc) would permit disclosure and section 13(1)(ee) would not be necessary. To avoid purely subjective interpretations of the meaning of "best interests" there should be criteria added to the Act to guide the assessment. Failure to include criteria could open the floodgates for disclosures of this personal information, which, given that it is about or relates to minors, is likely highly sensitive.

Recommendation

7. Regarding section 13(1)(ee), it is recommended that:

a. the section be modified to either require the consent of the individuals whose personal information is disclosed under this section or by adding at the end of this section "and obtaining the consent of the minor or their parent or guardian, as applicable, is unattainable or impracticable and disclosure is not against any expressed wish of the individual whose personal information is disclosed under this section"; and

b. who is responsible for determining "best interests" be specified in the section and criteria added in the section or elsewhere within PPA to guide the interpretation of "best interests".

PIA requirement dependency on regulations

Section 26 will only have effect once the circumstances under which a PIA must be completed are prescribed by regulation. PIAs will only need to be submitted to the Commissioner if prescribed. This section could be strengthened by setting out certain minimum requirements that trigger a duty to complete a PIA and for submitting the same to the Commissioner. PIAs should generally be required when sensitive personal information (e.g. biometric information or the personal information of minors or other vulnerable individuals) is compiled, when conducting data matching, when establishing common or integrated programs or services, regarding the disclosure of non-personal data where there is a risk of re-identification, and when automated decision-making takes place. PIAs should be submitted to the Commissioner whenever the activity involves risks to the public.

Recommendation

8. It is recommended that minimum requirements for creating a PIA and submitting the same to the Commissioner be added to section 26.

Privacy Management Programs

A privacy management program is commonly used to *ensure* privacy compliance of public bodies. Currently section 25(1) uses the term 'promote' which is a lower standard. As the Act applies to non-personal data and data derived from personal information, these terms should be added to section 25(2)(a).

Section 25(3) would benefit from a more proactive approach to accessibility such as making the program available in a publicly accessible location.

Section 25(5) creates a time gap between the introduction of the authority to match data and to collect, use or disclose personal information for common or integrated programs or services and the requirement for a public body to establish and implement a privacy management program under section 25(1). This creates a risk that a public body will engage in these activities without having gone through the efforts required to build a privacy management program, resulting in increased risks to the privacy

of Albertans. As such, a public body should be prohibited from engaging in these activities until they have implemented a privacy management program as required by section 25(1).

Given that the requirements with respect to privacy management programs will be prescribed, we strongly recommend having these requirements in place when section 25 comes into force, and that these requirements specify the minimum effort of the privacy management program, including the training of staff; creation of an inventory of personal information that the public body has custody or control of; risk management of that information based on sensitivity of the information; and assigning accountability and roles in regard to the program and risk management.

Recommendation

9. Regarding section 25, it is recommended that:

    a. section 25(1) be modified to require that public bodies establish and implement a privacy management program that will *ensure* compliance with PPA;

    b. section 25(3) requires public bodies to make their privacy management program available in a publicly accessible location by default;

    c. the ability of a public body to collect, use or disclose personal information for a common or integrated program or service or for data-matching be prohibited until the public body has met their obligations under section 25(1); and

    d. it is clarified (in the requirement to establish and implement a privacy management program) that the privacy management program must include training of staff, creation of an inventory of personal information that the public body has custody or control of, risk management requirements based on sensitivity of the information, and assigning accountability and roles regarding the program and risk management.

Automated decision-making

Section 5(2)(d) references the use of an automated system (AS) in relation to the duty to give notice for inputting personal information into an AS to generate content, or make decisions, recommendations or predictions. Section 6 also makes reference to an AS. It is unclear what "automated system" means and if it includes an automated decision-making system that also includes the use of artificial intelligence (AI). PPA would benefit from clarifying the meaning of "automated system".

I am surprised that PPA does not contain any protections for Albertans for the use of automated decision-making systems (ADM).

In the Sept 23/24 Letter and the Previous Report we made comments and recommendations about the protections for the use of ADM in previously-modernized privacy laws. These laws contain checks and

balances on the use of ADM where such use may produce adverse or significant effects for an individual, including requirements for transparency, accountability, recourse, opt-out or human intervention, and oversight. It is my view that adequate guardrails must be added to PPA to ensure Albertans are protected from the harms that could flow from the application of ADM or AI in administrative and government processes.

It is unclear in PPA if public bodies will be authorized to collect and use personal information to train AI. It is my view that any collection and use of personal information for this purpose be clarified so it is clear to Albertans that their personal information may be used for these purposes. There should also be the ability of Albertans to opt out of such collection or use. There should also be sufficient guardrails on this authority including transparency requirements for this activity.

The use of personal information to train and use generative AI must also consider that these systems may retain and reveal the original personal information. PPA must codify the risk mitigation measures that will protect Albertans from breaches of their personal information in the use of these systems.

Recommendation

10. It is recommended that PPA be amended to include adequate protections and rights for Albertans as it relates to the creation and use of ADM by public bodies.

Commissioner's powers

The Commissioner should be adequately empowered to give advice, investigate and monitor compliance regarding all provisions in PPA. To this end, we recommend the following.

Recommendation

11. It is recommended that the Commissioner be given the following powers under the Act:

    a. investigate compliance with any agreement entered into under the Act;

    b. request copies of privacy management programs (if not already made public);

    c. review and comment on a PIA and privacy management program of a public body;

    d. proactively audit a public body's compliance with the Act including with the security provisions, breach reporting procedures and training, and any prescribed requirements;

    e. audit compliance with this Act by any party;

    f. make any order that the Commissioner determines is necessary to enforce compliance with the Act.

Offence provisions

It is positive to see the increased fines under PPA. However, the amount of fines in PPA may not achieve the objective of deterring non-compliance and promoting compliance. The reasons for this are multi-factorial.

To date, the OIPC has only ever investigated potential offences under the *Health Information Act* (HIA). This is because the threshold in HIA is "knowingly", which differs from the higher offence threshold in the FOIP Act, which is "wilful". It is also because health information is highly sensitive and the OIPC has few resources to conduct these investigations.

The offence provisions in PPA are in section 60. The threshold for committing an offence is "knowingly", which now brings it in line with HIA. Under this section are offences for violating PPA, including for collecting, using or disclosing personal information contrary to Part 1, gaining or attempting to gain access to personal information in contravention of the Act, and others relating to data matching, data derived from personal information and re-identification of non-personal data. The fines are listed under sections 60(2) and (3). They are between $125,000 and $1,000,000. These are the highest fines under public sector privacy laws in Canada that I am aware of.

Offence provisions are generally included in law to deter non-compliance and to penalize violations of the law in certain specified purposes, which in turn acts as a deterrent. These provisions are only effective in achieving these objectives if:

- individuals who are subject to the law are aware of their responsibilities and the consequences of violating the law, and
- there are actual consequences for violating the law.

Alberta is one of the only Canadian jurisdictions where the Commissioner undertakes offence investigations as they are complex, resource-intensive and specialized. The OIPC has been conducting offence investigations under HIA since 2005. Under HIA, to date:

- 104 offences have been investigated;
- in 28 cases, charges were laid;
- in 22 cases, the person of interest was found guilty;
- in 20 cases, fines were levied; and
- with the exception of one, the fines levied for committing an offence ranged from $1,000 to $10,000, with the majority in the $3,000 to $5,000 range. Under HIA, the fine amounts associated with these offences are $200,000 in the case of an individual and $1,000,000 in any other case.

As can be seen, most of the fines levied for committing an offence under HIA are well below the maximum amounts outlined in that law, which limits the effectiveness of the deterrent factor. In addition, the following must also be considered.

- The Crown may decide not to proceed with a case based on certain criteria.
- Investigations are long and complex and take up to two years to complete.
- If the Crown lays charges, it can be years before the person of interest is in court.
- Most cases are settled without a court hearing.
- Even when a person is fined, the lack of contemporaneousness of the violation to the consequence means that those who may have been aware of the violation would often have no idea as to the outcome.

Even though there have been convictions and fines under HIA for unauthorized access to health information, snooping persists. It does not appear that the offence provisions are deterring non-compliance. It is questionable if the offence provisions are serving any real purpose under HIA.

For the offence provisions in PPA to have any value, the system designed to give life to these provisions must be adequately resourced and aligned.

- The OIPC must be adequately resourced to assess whether to investigate an offence and to investigate the same.
- The criteria used by the Crown to decide whether to lay charges must not take into account trivial factors to not proceed.
- Fines must be appropriate.
- Consequences must be communicated widely.

In 2024, due to lack of resources in my office to do this work, I declined to conduct 11 potential offence investigations under HIA and chose to conduct one systemic investigation instead.

Given our experience with HIA, we do expect there to be circumstances warranting offence investigations under PPA. The fact that there is mandatory breach reporting in PPA also sheds light on snooping, as will the privacy portal, if Albertans are able to review logs of access to their personal information, as alluded to by Minister Glubish.[7] The latter two factors will increase the likelihood that circumstances will be brought to our attention that warrant our opening offence investigations.

In the Previous Report and the Sept 23/24 Letter, we recommended that the Commissioner be authorized to issue administrative monetary penalties (AMPs) in certain circumstances. AMPs are now more common in privacy laws in recognition that they are immediate and impactful and more effective at deterring non-compliance and promoting compliance. To that end, we recommend the following:

[7] https://www.alberta.ca/release.cfm?xID=89657CD442215-F572-853B-1C2BC195593698A7

Recommendation

12. It is recommended that consideration be given to whether the offence provisions in PPA will effectively serve the purpose of deterring non-compliance and promoting compliance or if AMPs would be more effective.

Observations about other provisions in PPA

1. Section 1(n) defines non-personal data. The definition would be more useful, and allow for more adequate and granular protection, if divided between pseudonymized or de-identified information on the one hand, and anonymized information on the other. In the Previous Report, we described a framework governing the degrees to which information on the scale from personal information to anonymized data needs to be protected.

2. Some language used in the Act is vague to the point of being contrary to the principles of administrative law, i.e., plain language requirements, thereby creating ambiguity of jurisdiction and procedural fairness. Examples follow.

    - Section 3(1)(s)(iii) includes the wording '*is to be sent to a member'.* As this is arbitrary and built on mere intent, this provision creates a test that is unnecessarily vague. Wording such as '*is routinely sent to a member'* is much more tangible and testable.

    - PPA speaks in several provisions about a "reasonable person" or "reasonable" but there is no standard or definition of "reasonable" or "reasonable person" as it exists for example under the *Personal Information Protection Act* section 2 - Standard as to what is reasonable.

    - Section 5(2)(d) relies on *intention* at the time of collection. Intention is a very intangible concept that is hard to hold to a burden of proof. Intention can change at any given moment. Accordingly, notice regarding the use of an AS might not be given if there is no "intention" at the time of collection to input the information into an AS even though it may occur.

3. Regarding section 11, this provision is beneficial but should extend to data derived from personal information and any data where there is a risk of re-identification (derived and non-personal). Also, the meaning of "selling" should be defined to include all exchanges for remuneration or benefit, no matter the structure of the transaction.

4. When "information is available to the public" under section 13(1)(bb) should be defined in the Act or regulation.

5. Section 14(b) expands when a use or disclosure is consistent with the purpose of collection or compilation and will result in the un-siloing of personal information. At the very least, this authority

should be balanced with transparency requirements and limitations where this relates to sensitive information.

6. Section 15(b) authorizes a public body to disclose personal information to a person other than a public body for research purposes in certain specified circumstances, including for data matching, so long as the matching is not harmful to individuals and the benefits of the data matching are clearly in the public interest. To ensure decisions about when data matching can occur are not arbitrary, the Act should specify when the matching may be harmful and how the benefit is to be determined. Furthermore, section 15(c)(ii) would benefit from aligning with the non-identifying definitions used in the Act. Section 15(c)(iii) should apply to non-identifying information where a risk of re-identification remains.

7. Section 21(1) authorizes a public body to create non-personal data for the purposes described thereunder. Section 21(2) sets out that non-personal data must be created in accordance with generally accepted best practices and prescribed requirements for creating synthetic data or other types of non-personal data. To ensure accountability, consideration should be given to involving the Commissioner in the development of the best practices and the regulations to create synthetic data and other types of non-personal data.

8. Section 22 authorizes a public body to use non-personal data for any purpose. It is unclear why the authority for use is not connected to the purposes necessary to create non-personal data set out in 21(1).

9. Section 23 authorizes a public body to disclose non-personal data to another public body for any purpose and to a person other than a public body as described under section 23(1)(b). Section 23(1)(b(ii) and (iii) require that the head of the public body approve conditions of the disclosure including for security, prohibition on actual or attempts to re-identify, and requires that the head and the person to whom the non-personal data is being disclosed to, enter into an agreement. For the sake of transparency, consideration should be given to requiring the head to publish these agreements.

10. For clarity, section 29(5) should refer to records produced under subsections (1) to (3).

11. Regarding section 38(4), there can be circumstances in which the request cannot be made within the 60-day limit. As such, there should be a provision that allows a request for review to be delivered beyond the timelines in 38(4)(a) or (b) at the discretion of the Commissioner.

12. If the Commissioner's authority is expanded to include the ability to investigate compliance with any agreement entered into under the Act, section 39(1)(a) should be expanded to include *"to any person relevant to the request for review, who is subject to an agreement under this Act".*

13. The fine amount under section 52(6) is low to the point of being unlikely to deter the conduct described, regardless of the chance of proving the contravention.

14. Regarding section 60(2), consideration should be given to having reasonably high minimums in this provision, to avoid low fines which erodes the deterrent effect of these provisions.

15. In order to promote transparency, it would be beneficial under section 57 to require the creation of directories of data derived from personal information and non-personal data.

16. The lack of clear application of PPA to service providers of public bodies may create compliance gaps and risks to Albertans. The risks associated with service providers and my recommendations were included in the Previous Report and Sept 23/24 Letter.

Impact on the resources of the OIPC

While we are pleased to see the modernization of Alberta's public sector privacy law, PPA will have considerable impact on the work of the OIPC. To fulfill its regulatory function under this Act as set out therein, the OIPC must be adequately resourced for this work, or its role in the legislative scheme will not be effective in protecting the privacy of Albertans.