STANDING COMMITTEE ON ALBERTA'S ECONOMIC FUTURE

Discussion Guide:

The Personal Information Protection Act

The Standing Committee on Alberta's Economic Future

Ricardo Miranda (Chair)
MLA, Calgary-Cross (ND)

David A. Schneider (Deputy Chair)
MLA, Little Bow (W)

Shaye Anderson
MLA, Leduc-Beaumont (ND)

Jon Carson
MLA, Edmonton-Meadowlark (ND)

Michael Connolly
MLA, Calgary-Hawkwood (ND)

Craig Coolahan
MLA, Calgary-Klein (ND)

Lorne Dach
MLA, Edmonton-McClung (ND)

Maria Fitzpatrick
MLA, Lethbridge-East (ND)

Richard Gotfried
MLA, Calgary-Fish Creek (PC)

David B. Hanson
MLA, Lac La Biche-St. Paul-Two Hills (W)

Grant Hunter
MLA, Cardston-Taber-Warner (W)

Sandra Jansen
MLA, Calgary-North West (PC)

Colin Piquette
MLA, Athabasca-Sturgeon-Redwater (ND)

Kim Schreiner
MLA, Red Deer-North (ND)

Wes Taylor
MLA, Battle River-Wainwright (W)

TABLE OF CONTENTS

INTRODUCTION 4
WRITTEN SUBMISSIONS 5
ADDITIONAL INFORMATION 5
EXECUTIVE SUMMARY 6
FREEDOM OF EXPRESSION 8
THE PERSONAL INFORMATION PROTECTION ACT 10
Purpose 10
Application of PIPA 10
Exemptions to the Application of PIPA 10
THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT 12
PIPA and PIPEDA 12
CONSENT 13
Forms of Consent 13
Exceptions to Consent 14
Disclosure without a Warrant 14
ACCESS AND CORRECTION TO RECORDS CONTAINING PERSONAL INFORMATION 16
The Request Process 16
Fees for Access 17
Exceptions to Access 17
Mandatory Exceptions to Access 17
Discretionary Exceptions to Access 18
PERSONAL EMPLOYEE INFORMATION 19
Employment References 19
MANAGING PERSONAL RECORDS 20
Retention, Destruction, and Care of Personal Information 20
PERSONAL INFORMATION OUTSIDE OF CANADA 21
Policies and Practices for Service Providers 21
Notification about Service Providers 21
NOTIFICATION OF A BREACH OF PRIVACY 22
THE ROLE OF THE COMMISSIONER 23
OFFENCES 25
PROFESSIONAL REGULATORY ORGANIZATIONS 26
NON-PROFIT ORGANIZATIONS 27
OTHER COMMENTS 28
GLOSSARY 29
NOTES 31

INTRODUCTION

Alberta's *Personal Information Protection Act*, S.A. 2003, c. P-6.5, (known as "PIPA") aims to protect the personal information of customers, clients, and employees held by private sector organizations. The Act came into force on January 1, 2004, and has been amended several times since its inception.

Section 63(1) of the Act stipulates that a "special committee of the Legislative Assembly must begin a comprehensive review of the Act and the regulations made under it by July 1, 2015." This committee must submit a final report to the Legislative Assembly within 18 months after beginning its review, and the report "may include the special committee's recommendations for amendments to this Act, the regulations made under this Act or any other enactment."

On June 15, 2015, Government Motion 11 was agreed to by the Assembly. This motion designated the Standing Committee on Alberta's Economic Future as a special committee of the Assembly for the purpose of conducting a comprehensive review of PIPA pursuant to section 63 of that Act. On July 15, 2015, the Committee met to begin its review. The Committee's final report will be provided to the Legislative Assembly prior to the expiry of the 18-month timeline.

This discussion guide and questions are intended to serve as a starting point for those who make written submissions to facilitate consideration of the legislation and its implications.

The Office of the Information and Privacy Commissioner is the regulatory body for PIPA, and also the *Freedom of Information and Protection of Privacy Act* (FOIP) and the *Health Information Act* (HIA). This Committee's review, however, is restricted to PIPA and does not encompass matters governed by other legislation, including:

- Access and privacy issues relating to personal information in the custody or control of a public body that is subject to the *Freedom of Information and Protection of Privacy Act*.
- Access and privacy issues relating to individual health information within the scope of the *Health Information Act.*
- Access and privacy issues relating to information and organizations subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

For assistance in understanding a selection of the terms used in the Discussion Guide, please consult the glossary on pages 29 and 30.

WRITTEN SUBMISSIONS

This guide was developed as a starting point for interested parties to make written submissions to the Standing Committee on Alberta's Economic Future with respect to its review of the *Personal Information Protection Act*.

Your submission may be sent by email, mail, or facsimile to the address listed below. **An email attaching an electronic copy of your submission is preferred.** Anonymous submissions will not be considered. All submissions should be received by **February 26, 2016**.

Please send to:

Standing Committee on Alberta's Economic Future
c/o Jody Rempel, Committee Clerk
3rd Floor, 9820 -107 Street NW
Edmonton, AB T5K 1E7

Email: EconomicFuture.Committee@assembly.ab.ca

Fax: 780-427-5688

Please note that submissions will be publicly available on the Committee's website (assembly.ab.ca/committees/abeconomicfuture). Do not include any personal or confidential business information that you do not want to be made available to the public.

ADDITIONAL INFORMATION

Individuals and organizations seeking more information on the application of the *Personal Information Protection Act* can consult the websites of Service Alberta and the Office of the Information and Privacy Commissioner, which provide information on compliance with PIPA for businesses, non-profit organizations, and professional regulatory organizations.

The website for Service Alberta can be found at http://servicealberta.ca/pipa-overview.cfm. Individuals may also call the PIPA Information Line operated by Service Alberta at 780-644-7472 or pspinfo@gov.ab.ca; or toll free at 310-0000, then 780-644-7472.

The website of the Office of the Information and Privacy Commissioner can be found at https://www.oipc.ab.ca/.

EXECUTIVE SUMMARY

The Standing Committee on Alberta's Economic Future will consider your input in the preparation of its recommendations. The Committee's final report will be provided to the Legislative Assembly by December 2016, and will include a list of respondents.

The following questions can be found throughout the discussion guide to assist you in developing your response. Please read the relevant section of the discussion guide to receive context about each question.

1. **Are the provisions of the Act regarding the collection, use and disclosure of information by trade unions appropriate? Please explain why or why not and provide suggestions.**

2. **Should PIPA include additional exceptions to consent that would permit other kinds of organizations (i.e., other than trade unions) to collect, use or disclose personal information of individuals for purposes of free expression without those individuals' consent? If so, which kinds of organizations and for what types of free expression purposes?**

3. **Are the exemptions to PIPA appropriate?**

4. **Are the provisions dealing with forms of consent and the conditions attached to their use appropriate? Please explain why or why not and provide suggestions.**

5. **Does PIPA adequately support individuals who are unable to provide consent for the collection, disclosure and use of their personal information? Please explain why or why not and provide suggestions.**

6. **Are the exceptions to consent for the collection, use and disclosure of personal information appropriate? Please explain why or why not and provide suggestions.**

7. **Should the provisions of PIPA pertaining to disclosure without a warrant be changed? If so, what should be changed?**

8. **Should organizations be required to publish transparency reports on disclosures made without consent to public bodies and law enforcement agencies?**

9. **Are the processes for accessing records of personal information appropriate? Please explain why or why not and provide suggestions.**

10. **Are the provisions regarding fees for accessing records of personal information appropriate? Please explain why or why not and provide suggestions.**

11. **Should PIPA provide a fee structure for access to personal information? Please explain why or why not and provide suggestions.**

12. **Are the exemption provisions for refusing access to an individual's own personal information appropriate? Please explain why or why not and provide suggestions.**

13. **Are the provisions pertaining to personal employee information appropriate? Please explain why or why not and provide suggestions.**

14. **Are the provisions pertaining to employee references appropriate, or is more clarity needed about the information that may be disclosed in a reference? Please explain why or why not and provide suggestions.**

15. **Are the processes set out in PIPA for retaining, destroying, and caring for personal information appropriate? Please explain why or why not and provide suggestions.**

16. **Is the level of transparency required of organizations using third-party service providers outside of Canada sufficient? Please explain why or why not and provide suggestions.**

17. **Are the provisions of PIPA regarding notification of a breach of privacy appropriate? Please explain why or why not and provide suggestions.**

18. **Should the Commissioner's powers be changed or expanded? Please explain why or why not and provide suggestions.**

19. **Are the sections pertaining to offences functioning as intended and are they strong enough to deter breaches and actions in contravention of the Act? Please explain why or why not and provide suggestions.**

20. **Are the provisions in the Act regarding professional regulatory organizations appropriate? Please explain why or why not and provide suggestions.**

21. **Is the application of the Act to non-profit organizations appropriate, or should all non-profit organizations be subject to PIPA in all of their activities? Please explain why or why not and provide suggestions.**

22. **Do you have any other suggestions or comments regarding PIPA? Please comment on any topic relevant to PIPA not addressed by this discussion guide.**

The Standing Committee on Alberta's Economic Future thanks you for your input.

FREEDOM OF EXPRESSION

In response to a decision of the Supreme Court of Canada, PIPA was amended in December 2014.[1] The Supreme Court struck down PIPA in its entirety but suspended this declaration for one year to allow the Legislative Assembly of Alberta time to review the structure of the Act in relation to the issue of freedom of expression and decide how best to make the legislation constitutional.

The case at issue, *Alberta (Information and Privacy Commissioner of Alberta) v. United Food and Commercial Workers, Local 401,* originated in 2006 when the United Food and Commercial Workers, Local 401, representing workers at the Palace Casino in West Edmonton Mall, photographed and filmed individuals crossing their picket line while engaging in a legal strike. The Union posted signs indicating that images of people crossing the picket line might be placed on a website (*Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 410*, 2013 SCC 62, [2013] 3 S.C.R. 733 at para. 4). Several individuals captured in the images complained to the Information and Privacy Commissioner. As none of PIPA's exemptions permitted the Union to collect, use, and disclose personal information without consent for the purposes of advancing its interests in a labour dispute, an Adjudicator concluded that the Union's activities were not authorized. The case went through judicial review, then the Court of Queen's Bench of Alberta and Alberta Court of Appeal. The Alberta Court of Appeal found that PIPA restricted the Union's freedom of expression, and this was not justified as a reasonable limitation under section 1 of the *Canadian Charter of Rights and Freedoms*.[2] The Alberta Information and Privacy Commissioner appealed this decision to the Supreme Court of Canada in June 2013.

The Supreme Court considered whether PIPA "achieves a constitutionally acceptable balance between interests of individuals in controlling the collection, use and disclosure of their personal information and a union's freedom of expression."

In its ruling, the Supreme Court recognized the importance of "legislation which aims to protect control over personal information" and suggested that protection of privacy "should be characterized as 'quasi-constitutional' because of the fundamental role privacy plays in the preservation of a free and democratic society" (*Alberta v. UFCW*, SCC, at para. 19). The Supreme Court further acknowledged that "PIPA's objective is increasingly significant in the modern context, where new technologies give organizations an almost unlimited capacity to collect personal information, analyze it, use it and communicate it to others" [paragraph 20].

The court also found that "[t]he price PIPA exacts, however, is disproportionate to the benefits it promotes" (*Alberta v. UFCW*, SCC, at para. 25). Specifically, the Act did "not include any mechanism by which a union's constitutional right to freedom of expression may be balanced with the interests protected by the legislation" (*Alberta v. UFCW*, SCC, at para. 25).

"[O]f utmost significance," in the view of the Court "is that PIPA prohibits the collection, use or disclosure of personal information for many legitimate, expressive purposes related to labour relations. These purposes include ensuring the safety of union members, attempting to persuade the public not to do business with an employer and bringing debate on the labour conditions with an employer into the public realm" (*Alberta v. UFCW*, SCC, at para. 28).

While the Court did not "condone all of the Union's activities," it stated that "this infringement of the right to freedom of expression is disproportionate to the [Alberta] government's objective of providing individuals with control over personal information that they expose by crossing a picket line" (*Alberta v. UFCW*, SCC, at para. 37). The Court concluded that "[t]o the extent that PIPA restricted the Union's collection, use and disclosure of personal information for legitimate labour relations purposes, the Act violates s. 2(b) of the Charter[3] and cannot be justified under s. 1" (*Alberta v. UFCW*, SCC, at para. 38).

In response, the Legislative Assembly of Alberta enacted limited changes to PIPA in December 2014. PIPA was amended to clarify that a trade union could collect, use, and disclose personal information

without consent in limited circumstances concerning a matter of significant public interest or importance relating to a labour relations dispute involving the trade union (sections 14.1(1), 17.1(1), and 20.1(1)) if:

- the collection, use, and disclosure of personal information is reasonably necessary for that purpose (section 14.1(1)(a), 17.1(1)(a), and 20.1(1)(a)); and
- it is reasonable to collect, use and disclose the personal information without consent for that purpose, taking into consideration all relevant circumstances, including the nature and sensitivity of the information (sections 14.1(1)(b), 17.1(1)(b), and 20.1(1)(b)).

These provisions do not restrict or affect a trade union's ability to collect, use, or disclose personal information without consent in the specific circumstances outlined in the Act in sections 14, 17, and 20.

Section 62(1)(e.1) was added so that the Lieutenant Governor in Council may make regulations respecting the collection, use, and disclosure of personal information by trade unions under sections 14.1, 17.1, and 20.1 of the Act.

Section 62(1)(k) was similarly changed so that the Lieutenant Governor in Council may make regulations prescribing or otherwise determining whether or not personal information or personal information of a specific type comes within the meaning of the new provision, and if so how it should be treated as prescribed by the Act (section 62(2)(b)).

1. Are the provisions of the Act regarding the collection, use and disclosure of information by trade unions appropriate? Please explain why or why not and provide suggestions.

2. Should PIPA include additional exceptions to consent that would permit other kinds of organizations (i.e., other than trade unions) to collect, use or disclose personal information of individuals for purposes of free expression without those individuals' consent? If so, which kinds of organizations and for what types of free expression purposes?

THE PERSONAL INFORMATION PROTECTION ACT

PIPA came into effect on January 1, 2004, and aims to protect the personal information of an organization's customers, clients, and employees. Organizations have to follow the rules in the Act about collecting, using, and disclosing personal information and must look after the personal information that is in their custody or under their control. PIPA also gives individuals the right to ask an organization to see the personal information it has about them, to find out how it is being used and disclosed, and to ask for corrections if they believe a mistake has been made.

Purpose

The stated purpose of the Act is

> to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information in a way that is reasonable (section 3).

In its stated purpose and other provisions, PIPA uses a test of what is reasonable. This is defined as what a reasonable person would think is appropriate in a given circumstance (section 2).

Personal information is defined as "information about an identifiable individual" (section 1(1)(k)). This includes any information that can identify an individual, for example, name, address, telephone numbers, email addresses, age, date of birth, birthplace, physical appearance, weight, height, gender, marital status, race, ethnic origin, citizenship, blood type, medical history, DNA code, education, employment history, criminal history, income, financial history, purchases, spending habits, unique identification numbers, and account numbers.

PIPA's definition of personal information is intentionally broad in order to capture all forms of personal information and also account for new forms of technology which may create additional and unforeseen methods of identification.

Application of PIPA

PIPA applies to all organizations in respect of all personal information (section 4(1)). The definition of organizations in PIPA is broad. An organization is defined in section 1(1)(i) as

(i) a corporation,
(ii) an unincorporated association,
(iii) a trade union as defined in the *Labour Relations Code,*
(iv) a partnership as defined in the *Partnership Act*, and
(v) an individual acting in a commercial capacity,

but does not include an individual collecting, using, and/or disclosing personal information for their own personal or domestic purposes only.

Exemptions to the Application of PIPA

The broad applications of PIPA are mitigated by a number of very specific exemptions. PIPA does not apply to "public bodies," such as government departments, universities, public school boards, hospitals, and municipalities; the privacy legislation applicable to those organizations is the *Freedom of Information and Protection of Privacy Act,* R.S.A. 2000, c. F-25 (section 4(3)(e)). PIPA also does not apply to individual health information within the scope of the *Health Information Act*, R.S.A. 2000, c. H-5 (section 4(3)(f)).

Other exemptions are outlined in section 4(3). PIPA does not apply to the collection, use, or disclosure of personal information

- for artistic or literary purposes;
- for journalistic purposes;
- that is business contact information[4] when it is collected, used, or disclosed for the purpose of enabling the individual to be a contact in relation to his or her business responsibilities;
- by officers of the Legislature[5] as they carry out their duties;
- by or for a registered constituency association or registered party under the *Election Finances and Contributions Disclosure Act,* or in respect of an office or a position in a registered constituency association or a registered party;
- by or for a bona fide candidate for public office where the information is being collected, used, or disclosed for the purposes of campaigning.

PIPA also does not apply to personal information

- about an individual who has been dead for at least 20 years;
- about an individual who is contained in a record that has been in existence for at least 100 years;
- contained in any record that was transferred to an archival institution under specific circumstances;
- contained in a court file, a record of a judge of the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, or the Provincial Court of Alberta, a record of a master in chambers of the Court of Queen's Bench of Alberta, a record of a justice of the peace other than a non-presiding justice of the peace under the *Justice of the Peace Act*, a judicial administration record or a record relating to support services provided to the judges of any of the courts referred to in the clause;
- contained in a record that has been created by or for a Member of the Legislative Assembly or an elected or appointed member of a public body;
- by or for a registered constituency association or registered party or in respect of an office or a position in a registered constituency association or a registered party;
- contained in a personal note, communication, or draft decision created by or for a person who is acting in a judicial, quasi-judicial, or adjudicative capacity.

There are also instances in which non-profit organizations are partially exempted from PIPA, and this is discussed in the section on non-profit organizations in this guide.

Finally, PIPA is not to be applied so as to affect any legal privilege, limit information available by law to a party to a legal proceeding, or limit or affect the collection, use or disclosure of information that is the subject of trust conditions or undertakings to which a lawyer is subject (sections 4(5)(a), (b), (c)).

3. Are the exemptions to PIPA appropriate?

THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

PIPA is related to the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (known as "PIPEDA"). PIPEDA is federal legislation that sets ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

PIPA and PIPEDA

PIPA was found to be "substantially similar" to PIPEDA in 2004, and, as a result, PIPEDA does not apply to most organizations collecting, using, and disclosing personal information within Alberta.

Laws that are granted substantially similar designation by the federal government provide privacy protection that is equivalent or greater to the privacy protections that are found under PIPEDA. Substantially similar designation means that there is an exemption such that PIPEDA does not apply to the collection, use and disclosure of personal information by private-sector organizations within Alberta.

In Alberta, PIPEDA still governs the collection, use, and disclosure of private information by federal works, undertakings, and businesses, such as banks, telecommunications, and transport companies. There can also be situations where both PIPA and PIPEDA apply to an organization or to a transaction. Understanding the application of PIPA and PIPEDA can be complex. Consider the example of a retailer with stores in Alberta and Ontario. The retailer would have to comply with PIPA with respect to the personal information of its customers and employees in Alberta. The same company would have to comply with PIPEDA for its customers' personal information in Ontario. (PIPEDA does not apply to employees of provincially regulated organizations and so there would be no coverage for the retailer's employees in Ontario.)

CONSENT

PIPA establishes consent as the primary mechanism which individuals may use to control the collection, use, and disclosure of their personal information by organizations.

Forms of Consent

Except in circumstances specified by PIPA, an organization must obtain consent to collect, indirectly collect, use, and disclose personal information about an individual (section 7). The Act allows for three types of consent:

- express consent – consent given verbally or in writing, including via electronic communications (sections 8(1) and (5))
- implied or deemed consent – consent given voluntarily for a purpose that is reasonable and well understood, such as providing a name and telephone number when leaving items with a dry cleaner (sections 8(2), (2.1) and (2.2));
- consent by not opting out – consent that is deemed to have been granted if a reasonable opportunity to decline or object was provided but not acted upon (section 8(3)).

If an individual is incapacitated in some way, unable to provide consent, and power of attorney has been granted by the individual or a guardian has been appointed for the individual, the attorney, guardian or trustee may consent or decline consent for the collection, use, and disclosure of the individual's personal information (section 61(1)(e) and (g)).

Under PIPA, an organization may collect personal information only for particular purposes and only the information reasonably required to meet those purposes (sections 11(1) and (2)). Before or at the time of collecting personal information from the individual the information is about, the organization must give notice to the individual explaining the purposes for collection and the name of a person who can answer questions about the collection (section 13(1)). These notification provisions only apply when information is collected directly from an individual.

An organization cannot require an individual to consent to the collection, use, or disclosure of personal information as a condition of supplying a service or product, beyond what is necessary to provide the product or service (section 7(2)).

An individual may withdraw or vary consent by giving the organization reasonable notice (section 9(1)) as long as this withdrawal or variance does not prevent the individual or organization from meeting a legal obligation (section 9(5)).

An organization may not obtain consent to collect, use, or disclose information by deception (section 10).

4. Are the provisions dealing with forms of consent and the conditions attached to their use appropriate? Please explain why or why not and provide suggestions.

5. Does PIPA adequately support individuals who are unable to provide consent for the collection, disclosure and use of their personal information? Please explain why or why not and provide suggestions.

Exceptions to Consent

The Act contains limited and specific circumstances where personal information may be collected without consent (section 14), used without consent (section 17), and disclosed without consent (section 20).

For example, information may be collected, used, and disclosed without consent:

- if authorized or required by a statute or regulation of Alberta or Canada, a bylaw of a local government body, or a legislative instrument of a professional regulatory organization;
- if collection is from or the disclosure is to a public body that is authorized or required by an enactment of Alberta or Canada to disclose to or collect the information from the organization;
- if it is reasonable for the purposes of an investigation or legal proceeding; or
- to collect a debt owed to or repay a debt owed by the organization collecting, using, or disclosing that information.

In addition, information may be disclosed without consent, for example:

- for the purposes of complying with a subpoena, warrant, or order issued or made by a court;
- if necessary to respond to an emergency that threatens the life, health, or security of the individual or the public;
- for the purposes of preventing fraud, so long as the disclosure is to the Investigative Services division of the Insurance Bureau of Canada, or the Canadian Bankers Association, Bank Crime Division and Investigation Office, both empowered or recognized to prevent, detect, or supress fraud.

PIPA also has exceptions to consent for the collection, use, and disclosure of personal employee information (sections 15(1), 18(1), 21(1), (2)) discussed more fully in the Personal Employee Information section of this guide.

6. Are the exceptions to consent for the collection, use, and disclosure of personal information appropriate? Please explain why or why not and provide suggestions.

Disclosure without a Warrant

Section 20(f) of PIPA permits an organization to disclose personal information about an individual without consent if "the disclosure of the information is to a public body or law enforcement agency in Canada to assist in an investigation undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result." A 2014 decision of the Supreme Court of Canada referring to section 7(3)(c.1)(ii) of PIPEDA may have implications for this provision.

Section 7(3)(c.1)(ii) of PIPEDA provides that an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is "requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law." Section 20(f) of PIPA is a similar provision, and section 20(m) may potentially also allow disclosures without a warrant to law enforcement for an "investigation or legal proceeding".

In *R. v. Spencer* 2014 SCC 43, the Supreme Court examined the legality of an Internet service provider's voluntary disclosure of basic subscriber information (name, address, and phone number) to law enforcement officials. The request, made in writing and pursuant to section 7(3)(c.1)(ii) of *PIPEDA*, indicated that police were investigating an offence under the *Criminal Code*, R.S.C. 1985, c. C-46 and

that the subscriber information was being sought as part of an ongoing investigation. The police did not try to obtain a production order – the equivalent of a search warrant in this context – and were not required to do so by *PIPEDA* (*R. v. Spencer* 2014 SCC 43, [2014] 2 S.C.R. 212 at para. 11, 49).

The Court concluded that individuals have a right to be anonymous on the Internet.[6] The decision barred Internet service providers from voluntarily disclosing the names, addresses, and phone numbers of their customers to law enforcement officials in response to a request without a warrant. The Court ruled that the collection of subscriber information from an Internet service provider without a warrant, for the purpose of law enforcement, was contrary to the right of individuals under the *Canadian Charter of Rights and Freedoms* to be protected from unreasonable search and seizure without lawful authority and that a request from law enforcement does not constitute lawful authority.

In a statutory review of British Columbia's PIPA, completed in February 2015, the Special Committee to Review the Personal Information Protection Act in British Columbia considered the implications of the Supreme Court's decision for the provisions of B.C. PIPA. The Committee supported narrowing sections of B.C. PIPA that permit disclosure without a warrant because of the Supreme Court's decision and the possibility of a *Charter* challenge. The Committee also recommended that organizations should be required to document and publish transparency reports[7] on disclosures made without consent.[8]

7. Should the provisions of PIPA pertaining to disclosure without a warrant be changed? If so, what should be changed?

8. Should organizations be required to publish transparency reports on disclosures made without consent to public bodies and law enforcement agencies?

ACCESS AND CORRECTION TO RECORDS CONTAINING PERSONAL INFORMATION

The Request Process

As a result of the last Review of the Personal Information Protection Act, the provisions on access were amended to clarify the requirements for processing three types of requests that an individual may make with respect to their own information: a request for access, a request for information about use or disclosure, and a request for correction.[9]

PIPA permits an individual to make access, information and correction requests to an organization regarding their own personal information. There is no general right of access to an organization's records, only to an individual's own personal information. The individual can also request information about the purposes for which his or her personal information is being used, the circumstances of disclosure, and the names of persons to whom the personal information is being disclosed (section 24(1.2)).

If the applicant is unable to make a written access, information or correction request, an organization may provide him or her with an alternative means to make the request (*Personal Information Protection Act Regulation* A.R. 366/2003 [Regulation], section 10).

The Act guides how an organization must respond to an applicant. An organization must respond to an applicant if they have either custody (i.e., physical possession) or control (i.e., authority or ownership) of the records. An organization must respond to a request within 45 calendar days unless the time limit is extended. Time limits may be extended only in the particular circumstances set out in sections 28 and 31 of the Act. Failure of an organization to respond to a request is to be treated as a decision to refuse access (section 28(2.1)).

Where incorrect personal information has been disclosed to another organization, the organization must be notified of the correction. Correction is not mandatory but must be considered and where correction is not undertaken as a result of a correction request, the file must be annotated to reflect this.

If access is refused, the applicant must be provided with the reason as well as the name and address of a person who can answer questions about the refusal (section 29(2)(b)). The applicant must also be told that they can request a review of the refusal by the Information and Privacy Commissioner (sections 29(3)(c) and 46(1)).

Sometimes, as discussed on the next page, only part of a record is accessible to an applicant because specific exceptions apply. However, an organization must release as much of the record that pertains to the applicant as it can (section 24(4) and Regulation, section 9(2)).

The Information and Privacy Commissioner has the power to authorize an organization to disregard requests for access or correction that amount to an abuse of the right to make such requests (section 37).

9. Are the processes for accessing records of personal information appropriate? Please explain why or why not and provide suggestions.

Fees for Access

Reasonable fees for access may be charged, except in two circumstances: when an individual makes a request for correction (section 32(2)); and when a current, potential, or former employee requests access to personal employee information (section 32(1.1)).

In all other circumstances, an organization may charge an applicant a reasonable fee for access to his or her personal information or for information about the use or disclosure of that personal information (section 32(1)).

PIPA does not establish a fee schedule but stipulates that the fee must be 'reasonable'.

An organization charging a fee must provide a written estimate of the fee to the applicant (section 32(3)(a)). The applicant may be asked to pay a deposit before the access request is processed (section 32(3)(b)). The organization is not obliged to process an access or information request until the estimate has been accepted and the deposit, where required, has been paid (Regulation, sections 15(a) and (b)), nor is the organization obliged to provide access or information until the fees are paid in full (Regulation, section 17).

Where an organization has given an applicant a fee estimate and has not received a response within 30 days, the organization may consider the applicant's request to have been withdrawn (Regulation, section 16).

If an applicant disagrees with the fee, he or she may ask the Information and Privacy Commissioner to review the fee charged by an organization (section 36(2)(c)).

10. Are the provisions regarding fees for accessing records of personal information appropriate? Please explain why or why not and provide suggestions.

11. Should PIPA provide a fee structure for access to personal information? Please explain why or why not and provide suggestions.

Exceptions to Access

The Act allows an organization to refuse access to all or part of either a record or a request for information about use and disclosure in limited and specified circumstances. Other refusals are discretionary, allowing the organization to decide to release or withhold information.

Mandatory Exceptions to Access

Three exceptions specify the circumstances where an organization must refuse to grant an applicant access to their own personal information. An organization must refuse access if:

- disclosure could reasonably be expected to threaten the life or security of another individual (section 24(3)(a));
- the information would reveal personal information about another individual (section 24(3)(b)); or
- the information would reveal the identity of an individual who has in confidence provided an opinion about another individual and the individual providing the opinion does not consent to disclosure of his/her identity (section 24(3)(c)).

Discretionary Exceptions to Access

Six exceptions specify the circumstances under which an organization may refuse to grant an applicant access to their own personal information. An organization may refuse access if:

- the information is protected by legal privilege (section 24(2)(a));
- the disclosure would reveal confidential information that is of a commercial nature and it is not unreasonable to withhold that information (section 24(2)(b));
- the information was collected for an investigation or legal proceeding (section 24(2)(c));
- personal information of this kind would no longer be provided to the organization if the requested information was released and it is reasonable that the organization continues to receive such information (section 24(2)(d));
- the information was collected by a mediator or arbitrator or created in mediation or arbitration (section 24(2)(e));
- the information relates to or may be used by a Crown prosecutor in a court case (section 24(2)(f)).

12. Are the exemption provisions for refusing access to an individual's own personal information appropriate? Please explain why or why not and provide suggestions.

PERSONAL EMPLOYEE INFORMATION

PIPA applies to private sector organizations operating in Alberta and governs both personal information and personal employee information.

PIPA defines "employee" as a current employee – that is, an individual employed by an organization or who performs a service for an organization as a partner or director, officer or office holder, apprentice, volunteer, participant, or student (section 1(1)(e)).

The definition of "personal employee information" is somewhat broader and includes information about individuals who are current employees, potential employees, or former employees that is reasonably required by the organization for the purposes of establishing, managing, or terminating an employment or volunteer-work relationship, or managing a post-employment or post-volunteer-work relationship (section 1(1)(j)).

The Act allows an employer to collect, use, and disclose personal employee information without consent for reasonable purposes related only to recruitment, management, or termination of the employment or volunteer-work relationship, or managing the post-employment or post-volunteer work relationship (sections 15(1), 18(1), and 21(1) and (2)).

The employer must provide current employees with reasonable notification that their personal employee information is going to be collected, used, or disclosed and the purpose for this collection, use, or disclosure (sections 15(1)(c), 18(1)(c), and 21(1)(c)).

Finally, the general provisions of PIPA regarding personal information apply to personal employee information, including an employee's right to request access to and correction of his or her own personal information (sections 24 and 25). The employer must make a reasonable effort to ensure the information collected, used, or disclosed is accurate and complete (section 33), safeguarded against unauthorized access, modification, or destruction (section 34), and retained only for as long as reasonably required for business or legal purposes (section 35).

13. Are the provisions pertaining to personal employee information appropriate? Please explain why or why not and provide suggestions.

Employment References

PIPA specifies that an organization can disclose, without consent, personal information about a current or former employee to a current or potential employer but limits the information that may be disclosed in the reference.

The reference can only include personal employee information – that is, personal information that the organization collected for the purposes of establishing, managing, or terminating the employment or volunteer-work relationship between the organization and the individual. Furthermore, the disclosure of this information must be reasonable for the purpose of helping the employer determine the individual's eligibility or suitability for a position (section 21(2)).

14. Are the provisions pertaining to employee references appropriate, or is more clarity needed about the information that may be disclosed in a reference? Please explain why or why not and provide suggestions.

MANAGING PERSONAL RECORDS

While PIPA recognizes that there is a direct link between the protection of personal information and the management of records containing that information, the Act is not intended to govern records management processes within organizations.[10] Nevertheless, it contains provisions relating to the care, retention, and destruction of personal information that is in the custody of an organization or under its control. One possible concern is the length of time an organization retains personal information records.

Retention, Destruction, and Care of Personal Information

Personal information may be retained by an organization only for as long as the organization reasonably requires the information for a legal or business purpose (section 35(1)). When an organization no longer requires personal information for legal or business purposes, it must destroy or anonymize the records containing the information (sections 35(2)(a) and (b)).

Finally, an organization must make reasonable security arrangements to safeguard against risks in order to protect personal information that is in the organization's custody or under its control (section 34). Risks include unauthorized access, collection, use, disclosure, duplication, modification, disposal, or destruction.

15. Are the processes set out in PIPA for retaining, destroying, and caring for personal information appropriate? Please explain why or why not and provide suggestions.

PERSONAL INFORMATION OUTSIDE OF CANADA

During the last review of the Act in 2006-2007, the Select Special Personal Information Protection Act Review Committee considered the increasingly global nature of business and heard concerns that PIPA does not provide adequate protection for personal information transferred to a third-party service provider outside of Canada for collection, processing, or storage. To redress concerns arising from outsourcing to other jurisdictions, the Committee recommended that "the Act be amended to require organizations to notify individuals when they will be transferring the individuals' personal information to a third-party service provider outside Canada," and that "the federal government amend the *Personal Information Protection and Electronic Documents Act* to require organizations to notify individuals when they will be transferring the individuals' personal information to a third-party service provider outside Canada."[11]

PIPA defines service provider as any organization, including "a parent corporation, subsidiary, affiliate, contractor or subcontractor, that directly or indirectly provides a service for or on behalf of an organization" (section 1(1)(m.3)).

Policies and Practices for Service Providers

Section 6(1) of the Act requires all organizations collecting, using, or disclosing personal information to develop and follow policies and practices that are reasonable for the organization to meet its obligations under the Act, including policies and practices pertaining to the use of third-party service providers outside of Canada. If an organization uses a service provider outside of Canada, its policies and practices must include information regarding:

- the countries outside of Canada in which the collection, use, disclosure, or storage is occurring or may occur (section 6(2)(a)), and
- the purposes for which the service provider outside of Canada has been authorized to collect, use, or disclose personal information for or on behalf of the organization (section 6(2)(b)).

Written information about these policies and practices must be available upon request (section 6(3)).

Notification about Service Providers

PIPA requires that organizations provide affected individuals with notice if using a third-party service provider outside of Canada. Notification is required in two circumstances:

- when an organization in Alberta uses a service provider outside of Canada to collect personal information with consent (section 13.1(1)), and
- when an organization transfers the individual's personal information (collected with consent) to a service provider outside of Canada (section 13.1(2)).

This notification must be given before or at the time of the collection or transfer, and inform individuals about how they can obtain written information about the Alberta organization's policies and practices with respect to its use of third-party service providers outside of Canada (section 13.1(3)(a)), and the name, or position title of a person who is able to answer on behalf of the organization questions about the collection, use, disclosure, or storage of personal information by third-party service providers outside of Canada (section 13.1(3)(b)).

16. Is the level of transparency required of organizations using third-party service providers outside of Canada sufficient? Please explain why or why not and provide any suggestions for improvement.

NOTIFICATION OF A BREACH OF PRIVACY

Privacy breaches can have significant consequences for individuals, ranging from identity theft to humiliation and anxiety.

In 2006-2007, the Select Special Personal Information Protection Act Review Committee considered whether PIPA should be amended to require organizations to notify individuals when their personal information has been compromised, and how a notification should be enforced. The Committee reasoned that certain types of breaches, such as credit card information loss, will almost always pose an immediate and high risk to affected individuals, and that notification should be required in such situations.[12]

PIPA now requires an organization that suffers a loss or unauthorized access to or disclosure of personal information (breach) to notify the Information and Privacy Commissioner without reasonable delay if the breach poses a real risk of significant harm to affected individuals (section 34.1(1), Regulation, section 19). Failure to notify the Commissioner where a reasonable person would consider that there exists a real risk of significant harm is an offence under the Act (section 59(1)(e.1)). The Commissioner must have an expedited process to consider notice provided by the organization (section 37.1(3)).

PIPA does not define "real risk of significant harm."[13] To assist organizations reporting a breach of personal information, the Office of the Information and Privacy Commissioner offers a "Mandatory Breach Reporting Tool" on its website. The document defines real risk of significant harm according to the reasonable person test: for there to be a "real risk," a reasonable person would consider that some risk of damage, detriment, or injury may occur to the individual as a result of the breach. For the harm to be significant, it must be important and meaningful and have more than trivial consequences or effects.[14]

Once it has been determined that the breach poses a real risk of significant harm, the Commissioner may then require the organization to notify individuals affected by the breach and to do so within a specified period of time (section 37.1(1)). The notice to affected individuals must include:

- a description of the incident that led to the loss of unauthorized access or disclosure,
- the date or time when the incident occurred,
- a description of the personal information involved,
- information about any steps taken to reduce the risk of harm, and
- contact information for a person who can answer the individual's questions (Regulation, section 19.1).

The Commissioner may also require the organization to satisfy additional terms and conditions (section 37.1(2)), and the Commissioner has exclusive jurisdiction in the matter (section 37.1(6)).

It should be noted that these provisions do not restrict the ability of an organization to notify individuals on its own initiative, before or after notifying the Commissioner, even if the incident does not give rise to a real risk of significant harm (section 37.1(7)). If, however, the breach poses a real risk of significant harm and the organization notifies individuals in a way that does not meet the requirements of the Act and Regulation, the Commissioner may require the organization to provide further notification.

17. Are the provisions of PIPA regarding notification of a breach of privacy appropriate? Please explain why or why not and provide suggestions.

THE ROLE OF THE COMMISSIONER

The Act provides for independent oversight by Alberta's Information and Privacy Commissioner, who is also responsible for monitoring compliance with the *Freedom of Information and Protection of Privacy Act* (FOIP Act) and the *Health Information Act*. The Commissioner's role is set out in Parts 4 and 5 of PIPA. The Commissioner is specifically responsible for reviewing decisions made by organizations under the Act and generally responsible for monitoring how PIPA is administered to ensure that its purposes are achieved.

The Commissioner has the power to review the actions and decisions of organizations under PIPA. For example, the Commissioner can review or investigate:

- any decision, action, or failure to act by an organization regarding a request for access to or correction of an individual's own personal information (section 46(1));
- a complaint by an individual that an organization is improperly collecting, using, or disclosing personal information (sections 36(2) and 46(2));
- a complaint that an organization is not properly helping an applicant, or about the time taken to respond to a request or the fees charged (sections 36(2) and 46(2));
- a complaint that notification of a breach has not been provided in accordance with PIPA (sections 36(2) and 46(2)).

Investigations by the Commissioner may be initiated on the Commissioner's own initiative or in response to a complaint by an individual. The Commissioner may also jointly investigate matters with privacy commissioners in other Canadian jurisdictions (section 43.1).

A request for review or a complaint initiated by an individual must be made in writing and delivered to the Commissioner within the time periods specified in the Act (section 47). The review may determine whether the organization contravened PIPA and make constructive recommendations to improve the organization's compliance with the legislation. If the recommendations are accepted by the organization, and the matter is satisfactorily resolved on the part of the complainant, the matter is considered resolved and the complaint is closed.

The Commissioner can try to settle any matter under review or relating to a complaint using mediation (section 49), and can hold an inquiry (section 50) and issue orders that are binding on an organization (sections 52(6) and 53). The Commissioner can direct an individual to pursue another complaint resolution procedure before the Commissioner will deal with the matter (section 46(3)).

If the complainant is not satisfied, the organization chooses not to implement the recommendations offered, or resolution cannot otherwise be achieved, the Commissioner may conduct an inquiry into the matter in accordance with section 50(1) of PIPA. The Commissioner has discretion whether or not to hold an inquiry.

The Commissioner has broad powers in conducting investigations and inquiries (section 38). For example, the Commissioner can compel the production of records and examine those records even if the records are not subject to PIPA (sections 38(2), (3), and (4)).

Orders issued by the Commissioner may require specific action by an organization as provided by sections 52(2) and (3) of PIPA. For example, the Commissioner could direct the organization to give or refuse an individual access to records; require an organization to stop collecting, using, or disclosing personal information; or require an organization to destroy personal information obtained in contravention of PIPA.

The organization has 50 days to comply with the order (section 54), and failure to comply is an offence (section 59(1)(f)). The Commissioner may also file a copy of the order with the Court of Queen's Bench, at which time the order is enforceable as if it were an order or judgement of the Court (section 52(6)).

A party may apply to the Court of Queen's Bench for judicial review of an order (section 54.1). On judicial review, the Court may determine whether the Commissioner acted within the Commissioner's jurisdiction under PIPA.

18. Should the Commissioner's powers be changed or expanded? Please explain why or why not and provide suggestions.

OFFENCES

Privacy matters are generally disposed of under PIPA by review through mediation or inquiry. If the Commissioner thinks that an organization or individual has committed an offence, the Commissioner may refer the matter to the Crown for prosecution. According to section 59(1), an offence is committed if the person:

- collects, uses, or discloses personal information in contravention of Part 2 of the Act (provisions pertaining to consent as well as the collection, use, and disclosure of personal information);
- attempts to gain or gains access to personal information in contravention of the Act;
- disposes of, alters, falsifies, conceals, or destroys (or directs another person to do so) a record containing personal information or a record containing information about the use or disclosure of personal information
    - after receiving a request for access, or
    - in circumstances in which a reasonable person would consider a request for access likely to occur;
- obstructs the Commissioner in the performance of her duties;
- makes a false statement to the Commissioner;
- fails to provide notice of a breach to the Commissioner;
- takes employment action against an employee that discloses to the Commissioner information about contravention of PIPA; or
- fails to comply with an order made by the Commissioner under the Act (section 59(1)).

A person who commits an offence under the Act is liable to a fine of up to $10,000 in the case of an individual, and up to $100,000 in the case of an organization (section 59(2)). The Commissioner does not have authority to apply penalties or levy fines. Fines are assessed by an Alberta Provincial court judge following a conviction.

To date, there have been no charges laid pursuant to these sections in PIPA.

19. Are the sections pertaining to offences functioning as intended and are they strong enough to deter breaches and actions in contravention of the Act? Please explain why or why not and provide suggestions.

PROFESSIONAL REGULATORY ORGANIZATIONS

Section 55 of the *Personal Information Protection Act* contains provisions that enable professional regulatory organizations to balance the protection of personal information with their mandate to protect the public interest.

A professional regulatory organization (PRO) is an organization incorporated under a professional Act (section 1(1)(k.2)). PROs are generally self-governing professional or occupational bodies, incorporated under a statute that provides for the regulation of that profession or occupation. They regulate the standards of education and experience required of members to enter the profession or occupation, their standards of practice, continuing education requirements, and conduct of members. They also investigate and adjudicate complaints from the public or other members about alleged unprofessional conduct. Examples of professional regulatory organizations include the Law Society of Alberta and the Association of Professional Engineers and Geoscientists of Alberta (APEGA). There are currently over 40 PROs in Alberta.

A PRO has the option of following sections 1 to 35 of PIPA or deciding that its membership and the public would be better served by having a tailored personal information code. A personal information code must provide the same level of privacy protection as the Act but may offer additional or sector-specific privacy protection relevant to the public they serve and their members. A personal information code would govern the collection, use, and disclosure of personal information in a manner that is consistent with the purposes and intent of sections 1 to 35 of PIPA (section 55(1)(b)).[15] Such a code also allows a professional regulatory organization to address its unique concerns and outline its privacy protection measures using profession-specific wording and format.

In the event that a PRO wishes to operate under a personal information code, it must apply to the Minister for authorization to do so (Regulation, section 23(1)). The Minister may revoke that authorization, at which time the code would cease to be in effect (Regulation, section 26(3)(a)).

During the last review of PIPA, the Select Special Personal Information Protection Act Review Committee considered the role of PROs in Alberta, and the advantages and disadvantages of developing a personal information code within a professional regulatory organization. At the time there were no personal information codes in place for PROs in Alberta. The Committee recognized that it may be premature to make changes to provisions regarding the option of PROs to create personal information codes, and favoured maintaining the ability of PROs to address their concerns in a manner that does not affect other organizations subject to PIPA. The Committee recommended that "the issue of modifying or deleting these provisions be revisited during the next review of PIPA."[16]

To date, there are no PROs with personal information codes.

20. Are the provisions in the Act regarding professional regulatory organizations appropriate? Please explain why or why not and make suggestions.

NON-PROFIT ORGANIZATIONS

During the last review, the Select Special Personal Information Act Review Committee considered whether PIPA should be amended to change the way the Act applies to non-profit organizations. It was considered that the definition of non-profit organization has resulted in different treatment of similar organizations under the Act (i.e., not-for-profit organizations that fall within the definition and those that do not). The Committee heard that some respondents were concerned that requiring all organizations within the non-profit sector to comply with PIPA would strain the resources of these organizations. Other respondents favoured full inclusion under the Act of all organizations in the non-profit sector in order to bring clarity and consistency, and ensure the protection of personal information held by these organizations.

Committee members favoured an approach that would provide certainty as to who is covered under the Act. At the same time, the Committee recognized that complying with PIPA might result in an administrative burden, especially for small- and medium-sized organizations and volunteer organizations in the non-profit sector. The Committee therefore recommended that "the Act be amended to make PIPA apply fully to all not-for-profit organizations, subject to a one-year transition period."[17] This recommendation was not implemented.

Consequently, PIPA continues to apply to all provincially regulated organizations in Alberta, but there are special provisions for certain non-profit organizations that:

- are incorporated under the *Societies Act,*
- are incorporated under the *Agricultural Societies Act,*
- are registered under Part 9 of the *Companies Act*, or
- meet the criteria established under the regulations to qualify as a non-profit organization (section 56(1)(b)).

These non-profit organizations are not required to follow the rules set out in the Act when collecting, using, or disclosing personal information (section 56(2)), except when they engage in a commercial activity.

"Commercial activity" means any transaction, act, or conduct or any regular course of conduct that is of a commercial character (section 56(1)(a)). This includes:

- selling, bartering, or leasing membership, donor, or other fundraising lists;
- the operation of a private school or an early childhood services program as defined in the *School Act*; and
- the operation of a private college as defined in the *Post-secondary Learning Act* (section 56(1)(a)).

Many non-profit organizations hold collections of sensitive personal information. Some may choose to develop and follow a privacy policy and the general principles of PIPA on a voluntary basis, but these voluntary practices are not subject to review by the Commissioner, nor are these organizations required to report breaches to the Commissioner.

Other organizations may also operate on a not-for-profit basis. However, if these organizations are otherwise incorporated and do not meet the definition of non-profit organization under section 56 of PIPA, these organizations must fully comply with the entire Act for handling the personal information of their employees, volunteers, clients, and donors.

21. Is the application of the Act to non-profit organizations appropriate, or should all non-profit organizations be subject to PIPA in all of their activities? Please explain why or why not and provide suggestions.

OTHER COMMENTS

22. Do you have any other suggestions or comments regarding PIPA? Please comment on any topic relevant to PIPA not addressed by this discussion guide.

GLOSSARY

Act: a written ordinance of a parliament or other legislative body.

Anonymize: the action of making anonymous, especially by the removal of names or identifying particulars.

Commercial: of, engaged in, or concerned with commerce.

Commercial activity: PIPA defines "commercial activity" as any transaction, act or conduct, or any regular course of conduct that is of a commercial character and, without restricting the generality of the foregoing, includes the following: the selling, bartering or leasing of membership lists or of donor or other fund-raising lists; the operation of a private school or an early childhood services program as defined in the *School Act;* the operation of a private college as defined in the *Post-secondary Learning Act* (section 56(1)(a)).

Consent: to express willingness, give permission, agree.

Disclosure: the act or instance of disclosing (making known, revealing).

Employee: PIPA defines employee as an individual employed by an organization and includes an individual who performs a service for or in relation to or in connection with an organization as a partner or a director, officer or other office-holder of the organization; as an apprentice, volunteer, participant or student; or under a contract or an agency relationship with the organization (section 1(1)(e)).

Employer: a person who employs another to undertake a task, carry out work, etc.

Exemption: exclusion from participation.

Jurisdiction: the extent or range of judicial or administrative power; the extent over which such power extends.

Legislation: a law or series of laws.

Non-profit Organization: PIPA defines non-profit organization as an organization that is incorporated under the *Societies Act* or the *Agricultural Societies Act,* or that is registered under Part 9 of the *Companies Act*, or that meets the criterial established under the regulations to qualify as a non-profit organization (section 56(1)(b)).

Notification: the action of informing or giving notice (declaring an intention).

Organization: PIPA defines organization as including a corporation, an unincorporated association, a trade union as defined in the Labour Relation Code, a partnership as defined in the *Partnership Act*, and an individual acting in a commercial capacity, but does not include an individual acting in a personal or domestic capacity (section 1(1)(i)).

Personal employee information: PIPA defines personal employee information as, in respect of an individual who is a potential, current or former employee of an organization, personal information reasonably required by the organization for the purposes of establishing, managing or terminating an employment or volunteer-work relationship; or managing a post-employment or post-volunteer-work relationship between the organization and the individual, but does not include personal information about the individual that is unrelated to that relationship (section 1(1)(j)).

Personal information: PIPA defines personal information as information about an identifiable individual (section 1(1)(k)).

Personal information code: PIPA defines personal information code as a code governing the collection, use and disclosure of personal information in a manner that is consistent with the purposes and intent of sections 1 to 35 of PIPA (section 55(1)(b)).

Professional Regulatory Organization: PIPA defines professional regulatory organization as an organization incorporated under a professional Act (section 1(1)(k.2)).

Reasonable: PIPA defines reasonable as what a reasonable person would think was appropriate in the circumstances (section 2).

Record: PIPA defines record as a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or any other form, but does not include a computer program or other mechanism that can produce a record (section 1(1)(m)).

Reference: a testimonial supporting an applicant for employment.

Regulation: a subordinate form of legislation that may be established without the necessity of enacting a new statute.

Service provider: PIPA defines service provider as any organization, including without limitation, a parent corporation, subsidiary, affiliate, contractor or subcontractor that directly or indirectly, provides a service for or on behalf of another organization (section 1(1)(m.3)).

Supreme Court of Canada: the highest court in Canada for all legal issues of federal and provincial jurisdiction.

Union Member: an individual belonging to a trade union.

Warrant: a written authorization authorizing police to search premises, arrest a suspect, etc.

NOTES

[1] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 410*, 2013 SCC 62, [2013] 3 S.C.R. 733.
[2] Section 1 of the Canadian Charter of Rights and Freedoms "guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."
[3] Section 2(b) of the Canadian Charter of Rights and Freedoms states that everyone has the "freedom of thought, belief, opinion and expression, including the freedom of the press and other media communication".
[4] Business contact information is defined by PIPA as an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information (section 1(1)(a)).
[5] The Officers of the Legislature are: the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, the Information and Privacy Commissioner, the Child and Youth Advocate, and the Public Interest Commissioner.
[6] *R. v. Spencer* 2014 SCC 43, [2014] 2 S.C.R. 212.
[7] Transparency reports are statistics issued by companies at regular intervals that disclose, for example, the number of times the company has complied with government or law enforcement requests for users' account information.
[8] British Columbia, Legislative Assembly, Special Committee to Review the *Personal Information Protection Act*, "Report of the Special Committee to Review the *Personal Information Protection Act*," (February 6, 2015), pp. 22.
[9] Alberta, Service Alberta, "Information Sheet 10: Personal Information Protection Amendment Act, 2009, April 2010," p. 7 available at: http://servicealberta.ca/pipa/documents/infosheet10.pdf
[10] Alberta, Legislative Assembly, Select Special PIPA Review Committee, "Select Special PIPA Review Committee Final Report, November 2007," (November 2007), p. 32.
[11] Ibid., p. 7.
[12] Ibid., pp. 8-9.
[13] Recent amendments to PIPEDA define "significant harm" as including "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property" (PIPEDA, section 10.1(7)). PIPEDA further states that the factors relevant to determining whether a breach of security safeguards creates a real risk of significant harm include, "(a) the sensitivity of the personal information involved in the breach; (b) the probability that the personal information has been, is being or will be misused; and (c) any other prescribed factor" (PIPEDA, section 10.1(8)).
[14] Office of the Information and Privacy Commissioner, "*Personal Information Protection Act* Mandatory Breach Reporting Tool," pp. 4-5. http://www.oipc.ab.ca/Content_Files/Files/Publications/Mandatory_Breach_Reporting_Tool_2012.pdf
[15] Sections 1 to 35 cover compliance and policies, consent, collection, use, disclosure, business transactions, access and correction and care of personal information.
[16] Alberta, Legislative Assembly, Select Special PIPA Review Committee, "Select Special PIPA Review Committee Final Report, November 2007," (November 2007), p. 31.
[17] Ibid., p. 11.