

REVIEW OF THE PERSONAL INFORMATION PROTECTION ACT



Final Report

November 2007



COMMITTEES
OF THE LEGISLATIVE ASSEMBLY

Select Special Personal Information
Protection Act Review Committee

Select Special Personal
Information Protection Act
Review Committee

Final Report

November 2007



Select Special Personal Information
Protection Act Review Committee
801 Legislature Annex
9718 – 107 Street
Edmonton, Alberta T5K 1E4
karen.sawchuk@assembly.ab.ca

Message from the Chair

Alberta today is an exciting place to live, work and do business. We have vibrant communities, a highly educated work force and dynamic entrepreneurs. We are connected to each other and to the world.

Albertans are open to new ideas and new ways of doing things. We have embraced new information technologies to meet our personal and business needs.

Technology has expanded options and opportunities. Citizens are able to access goods and services in ways that could scarcely have been imagined a decade ago. Businesses are able to compete successfully in local and global markets.

At the same time, Albertans are sophisticated consumers. They value the convenience of online access to goods and services, and the efficiencies that information technologies bring, but they also value their privacy.

Whether they are shopping, applying for a job, taking a course, or registering their children in recreational programs, they want to do it within a relationship of trust. Albertans want to be sure that the organizations to which they give their personal information will protect that information. They are aware of the amount of personal information some organizations gather about individuals. And they are aware of the risks this can create.

Organizations in Alberta understand that privacy protection is valued by their customers, clients and employees. They know that sound privacy protection makes good business sense.

In 2004, Alberta made a bold move. Instead of allowing federal legislation to govern privacy in the Alberta private sector, the Province introduced its own privacy legislation. Alberta's *Personal Information Protection Act* (PIPA) was designed to provide the legal framework to support relationships of trust between individuals and organizations.

PIPA has established a set of sound, common-sense rules for the collection, use, disclosure, and protection of personal information by organizations. The Act gives Albertans strong, effective privacy protection.

During this first review of the Act, the Select Special Review Committee, which we were honoured to chair, heard that PIPA is working well. It has struck the right balance between the rights of individuals to have their personal information protected, and the needs of organizations to collect, use and disclose personal information of their clients and employees for reasonable purposes.

It is clear that innovations in PIPA, such as the special rules for protecting the personal information of employees and for protecting personal information when a business is sold, have been a great success.

The main proposals for change in this Report concern emerging issues, such as notifying individuals about security breaches that place personal information at risk, and protecting personal information when it moves outside the borders of Alberta.

As with any new legislation in a rapidly evolving area, some updating and fine tuning is required. We want to ensure that PIPA keeps pace with growth and change, and that it will serve Albertans well into the next decade.

Cindy Ady, MLA
Chair, Select Special PIPA Review Committee

George VanderBurg, MLA
Deputy Chair, Select Special PIPA Review Committee

HIGHLIGHTS OF THE REPORT

Private-sector privacy was a relatively new concept in Canada when Alberta's *Personal Information Protection Act* (PIPA) came into force on January 1, 2004. Recent federal legislation provided a model, but some significant changes were incorporated into the provincial statute. The response has generally been positive.

However, as with all new ventures, there is room for improvement. A little more than three years of operation has revealed several areas where PIPA can be enhanced.

This report presents 39 recommendations for changes to allow the Act to evolve and more effectively respond to the needs of Albertans, rapid advances in technology and emerging privacy issues.

● Key recommendations

For each recommendation the Committee recognized the importance of maintaining harmony with other private-sector privacy legislation in Canada, while retaining those unique provisions that allow PIPA to respond directly to the concerns of Alberta organizations and individuals.

Require organizations to inform individuals of transborder flows of their personal information

Require organizations to notify individuals when they will be transferring personal information to a third-party service provider outside Canada (Recommendation 1).

Create a new duty for notification of privacy breaches

Provide a framework within the Act for organizations to report certain privacy breaches to the Office of the Information and Privacy Commissioner and, if necessary, affected individuals, as well as an offence provision for failure to report a breach (Recommendations 3 and 4).

Bring all not-for-profit organizations fully within the scope of the Act

Ensure that employees, volunteers and clients of all not-for-profit organizations receive the same privacy protection as employees, volunteers and clients of other organizations in Alberta (Recommendation 5).

Provide privacy protection for health-related personal information under HIA rather than PIPA

Recommend to the Minister of Health and Wellness that all personal information related to treatment and care in a health care setting be brought within the scope of the *Health Information Act* (HIA), while ensuring that personal information can continue to flow between custodians and organizations where necessary (Recommendations 7 and 8).

Clarify the rules governing personal employee information

Expand the scope of the personal employee information provisions to clearly include former employees. Require an organization to obtain consent to collect, use and disclose employment references (Recommendations 18 and 19).

Revise consent provisions to better address longstanding business practices

Enable organizations to obtain consent through an intermediary; facilitate processes for group or family enrolment in insurance and benefit plans; allow organizations to perform audits and inspections that include personal information (Recommendations 9, 10 and 12).

Create time limits for the retention of personal information

Require an organization to destroy personal information that an organization no longer requires for legal or business purposes, within a reasonable time. Require an organization to retain records relating to a Commissioner's investigation for a year after the investigation (Recommendations 29 and 30).

Establish new offence provisions

Enable the Crown to prosecute violations of the Act's "whistleblower" protection provisions, and the concealment of evidence during a Commissioner's investigation or inquiry (Recommendations 42 and 43).

Establish more appropriate standards for prosecuting offences

Change the standard required to find an offence under the Act from intentional to negligent, and increase the time limit to prosecute offences from six months to two years (Recommendations 44 and 45).

Streamline Commissioner's processes and clarify powers

Allow the Commissioner to discontinue investigations into complaints that lack merit or sufficient evidence; clarify that disclosing information protected by solicitor-client privilege to the Commissioner at his request does not affect that privilege; allow the Commissioner to disclose information relating to the commission of an offence to the Minister of Justice and Attorney General (Recommendations 32, 33 and 34).

CONTENTS

MANDATE	1
ACKNOWLEDGEMENTS	2
ABOUT THE PERSONAL INFORMATION PROTECTION ACT	3
THE PUBLIC CONSULTATION PROCESS	4
COMMITTEE RECOMMENDATIONS	5
❶ Consistent approach to privacy legislation.....	5
❷ Processing personal information outside Canada	6
Notice of and consent to transfer personal information outside Canada.....	6
❸ Notification of a breach of privacy.....	8
Inclusion of a breach notification provision.....	8
Enforcement of the notification provision.....	9
❹ Non-profit organizations.....	10
Application of PIPA to non-profit organizations	10
Disclosure of membership lists by religious organizations.....	11
❺ Health information.....	13
Scope of PIPA and the Health Information Act	13
Interaction between PIPA and HIA.....	14
❻ Forms of consent	15
Indirect collection through an intermediary organization	15
Indirect collection for group and family insurance and benefit plans	16
Requirements for notification.....	17
❼ Exceptions to consent.....	18
Audits and inspections.....	18
Fraud prevention.....	19
Notification for collection of personal information.....	19
Regulation-making powers.....	20
Business contact information	20
Publicly available personal information.....	21
“Officer of the Legislature”.....	21
❽ Personal employee information	22
Application of PIPA to former employees	22
Employee references	23
Definition of an “employee”	23
Limitations on the collection, use and disclosure of personal information.....	24
❾ Access to records containing personal information	25
Continuing requests.....	25
Work product information.....	25

Failure of an organization to respond to an access request	26
● Exceptions to access	27
Confidential information of a commercial nature	27
Records subject to a solicitor’s lien	27
● Fees	29
Fee schedule	29
Waiver of fees	29
Fees for correcting personal information	30
● Professional regulatory organizations	31
Personal information codes	31
● Managing personal information	32
Retention of personal information	32
Retention period for records relating to a Commissioner’s investigation	33
Accuracy of personal information	33
● The independent review	34
Early dismissal of complaints and requests for review	34
Solicitor–client privilege	35
No waiver of privilege	36
Disclosure of evidence of an offence to the Minister of Justice and Attorney General	36
Time limits for inquiries	37
Audit powers	38
Power to enter premises	38
Commissioner as a compellable witness	39
Judicial review process	39
Duty to make an order	40
Access to recorded personal information	41
Notification of a review or complaint	41
● Offences and penalties	42
Failure to make reasonable security arrangements	42
Contravention of “whistleblower” protections	42
Destruction, alteration, falsification, or concealment of evidentiary records	43
Prosecution of PIPA offences	43
Time limits for prosecutions	44
Penalties under PIPA	44
● Administration of the Act	46
Review of the Act	46
Relation between the Act and the Regulation	46
Appendix A: Submissions to the Review Committee	47
Appendix B: Oral presentations to the Review Committee	49
Appendix C: Recommendations	50

MANDATE

On May 16, 2006, the Legislative Assembly of Alberta passed a motion appointing an all-party Committee to review the *Personal Information Protection Act*. The mandate of the Committee was to determine whether the Act and its supporting regulation and policy provide an appropriate balance between the right of an individual to have his or her personal information protected and an organization's need to collect, use and disclose personal information for purposes that are reasonable. The Committee was charged with providing to the Assembly, within 18 months after beginning the review, a report that includes any recommended amendments.

A key element to business success is building employee and customer confidence and loyalty, which is the basis of sound privacy practices.

IBM CANADA LTD.

On March 8, 2007, the Assembly passed a motion changing the Committee's membership.

The Committee consists of:

- Mrs. Cindy Ady, Calgary–Shaw (Chair)
- Mr. George VanderBurg, Whitecourt–Ste. Anne (Deputy Chair), replacing Mr. Hector Goudreau, Dunvegan–Central Peace (Deputy Chair)
- Ms Laurie Blakeman, Edmonton–Centre, replacing Mr. Dan Backs, Edmonton–Manning
- Mr. David Coutts, Livingstone–Macleod, replacing Mr. Art Johnston, Calgary–Hays
- Mr. Denis Ducharme, Bonnyville–Cold Lake, replacing Mr. Ron Liepert, Calgary–West
- Mr. Gordon Graydon, Grande Prairie–Wapiti, replacing Mr. Fred Lindsay, Stony Plain
- Mr. Ty Lund, Rocky Mountain House, replacing Mr. Rob Lougheed, Strathcona
- Mr. Hugh MacDonald, Edmonton–Gold Bar
- Mr. Ray Martin, Edmonton–Beverly–Clareview
- Mr. Barry McFarland, Little Bow, replacing Mr. Dave Rodney, Calgary–Lougheed
- Mr. Len Webber, Calgary–Foothills, replacing Mr. Lloyd Snelgrove, Vermilion–Lloydminster

As individuals, how can we proactively protect ourselves if we are unaware our information has been breached?

INDIVIDUAL

Any changes which promote consistency between the various pieces of privacy legislation applicable in Alberta would be welcome.

ALBERTA
BLUE CROSS

ACKNOWLEDGEMENTS

Non-profit organizations should be held to the same standard of protection of privacy as organizations, regardless of whether they are participating in commercial activities.

ARMA – CALGARY
CHAPTER

By clarifying the scope of PIPA and ensuring that health information does not fall under its rules and processes, we can ensure a more level playing field for health information and increased comfort for patients.

ALBERTA MEDICAL
ASSOCIATION

Organizations should be required to notify individuals when specific types of personal information have been breached.

ALBERTA
TEACHERS'
ASSOCIATION

The Committee wishes to acknowledge the many Albertans who submitted written briefs and letters or appeared before the Committee for their valuable contributions to this important process.

The Committee also wishes to acknowledge the valuable assistance of the technical support staff.

Technical Support Team

- Mr. Tom Thackeray, Service Alberta
- Ms Hilary Lynas, Service Alberta
- Ms Jann Lynn-George, Service Alberta
- Ms Kim Kreutzer Work, Service Alberta
- Ms Amanda Swanek, Service Alberta
- Ms Elizabeth Denham, Office of the Information and Privacy Commissioner
- Ms Jill Clayton, Office of the Information and Privacy Commissioner

Support Staff

- Mrs. Karen Sawchuk, Legislative Assembly of Alberta
- Ms Rhonda Sorenson, Legislative Assembly of Alberta
- Ms Tracey Sales, Legislative Assembly of Alberta
- *Hansard* Staff, Legislative Assembly of Alberta

ABOUT THE PERSONAL INFORMATION PROTECTION ACT

The introduction of Alberta's *Personal Information Protection Act* (PIPA) on January 1, 2004 was a response to the changing nature of privacy in today's world. Privacy had long been characterized as a "right to be let alone." However, dramatic advances in technology and the increasingly global dimension of both business and social connections have led to a shift in the way privacy is perceived. "Informational privacy" – the ability to control one's own personal information – has come to dominate the conversation on privacy.

Hailed as "second-generation" legislation, PIPA was based on federal private-sector privacy legislation that came into force in stages from 2001 to 2004. Had Alberta not enacted its own legislation, the federal Act would have applied within the Province. It was felt that the interests of individuals and organizations in Alberta required a distinct and innovative approach: an Act made *in Alberta, for Albertans*.

PIPA sets rules for organizations operating in Alberta with respect to the collection, use and disclosure of personal information regarding their customers, clients and employees. An individual's right to have his or her personal information protected is balanced against an organization's need to collect, use and disclose personal information for reasonable purposes. The Act gives an individual the right to ask an organization for access to his or her personal information held by that organization, with some exceptions.

As a new Act developed to address a changing conception of privacy, rapidly evolving technologies and new global realities, it was important that PIPA be subject to a comprehensive review within a few years of its introduction. The Act established a requirement that a special committee of the Legislative Assembly begin a review by July 1, 2006, and at least once every three years after that. The special committee must submit a report to the Legislative Assembly within eighteen months of beginning a review.

This final report presents the recommendations of the all-party Legislative Assembly Committee after its deliberations on the written submissions received and oral presentations heard during the consultation process.

The proceedings of the Select Special Personal Information Protection Act Review Committee are recorded in *Hansard* and are available online at www.assembly.ab.ca.

Alberta PIPA is the "best-in-sector" statute.

CANADIAN BAR
ASSOCIATION -
ALBERTA

In today's global economy, sending personal information outside of Canada for processing or storage is a business reality; in the interest of business efficacy, to refuse to do so is not an option.

ATB FINANCIAL

Access to the Office of the Privacy Commissioner and to compliance assistance has been helpful to small and medium-sized businesses.

CANADIAN
FEDERATION OF
INDEPENDENT
BUSINESS

THE PUBLIC CONSULTATION PROCESS

PIPA is working and doing its job for Albertans. No reason has been identified that would require PIPA to change.

INDEPENDENT
INSURANCE
BROKERS
ASSOCIATION
OF ALBERTA

The biggest challenge faced by retailers related to the collection of customers' personal information is most definitely at the returns desk.

RETAIL COUNCIL
OF CANADA

If an individual chooses to participate in employer benefit plans ... there [should be] deemed consent for the collection, use and distribution of personal information for the purpose of administering ... those benefit plans.

SYNCRUDE
CANADA LTD.

In July 2006, a Discussion Guide was distributed to help Albertans contribute to the review process. The Guide was distributed to more than 362 organizations. Sixty-five submissions were received by the Committee. Of these, twenty-four came from industry and business or professional associations, eighteen were from individual organizations, thirteen were from professional regulatory organizations, and seven were from individuals. Of the respondents, eighteen were identified as non-profit organizations under PIPA. Twenty respondents were identified as organizations with head offices outside Alberta which operate under both PIPA and federal private-sector privacy legislation. Submissions were also received from the Information and Privacy Commissioner, Service Alberta (the ministry responsible for the administration of the Act), and the Personal Information Protection Act Advisory Committee.

A list of individuals and organizations that provided written submissions to the Committee is presented in Appendix A.

In addition to receiving written submissions, the Committee heard ten oral presentations from various organizations and individuals, including the Office of the Information and Privacy Commissioner and Service Alberta. A list of individuals and organizations that provided oral presentations to the Committee is presented in Appendix B.

The Committee considered responses to questions in the Discussion Guide as well as other issues raised by respondents in written submissions and oral presentations. In reaching its recommendations on these issues, the Committee took into consideration comments from the public, information provided in various briefings and policy option papers, and information requested by Committee members in the course of its proceedings. The Final Report includes a summary of the Committee's deliberations and its final recommendations.

All recommendations made by the Committee, as well as issues on which the Committee decided not to make a formal recommendation, are listed in Appendix C.

COMMITTEE RECOMMENDATIONS

● Consistent approach to privacy legislation

In 2003, Alberta decided to introduce its own private-sector privacy legislation, rather than allowing the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) to apply to Alberta organizations. Alberta worked with British Columbia to develop legislation that would be similar to the federal PIPEDA, but simpler and better suited to the needs of small and medium-sized businesses.

In the course of the first review of Alberta's new *Personal Information Protection Act* (PIPA), the Select Special Committee heard that organizations and individuals are generally pleased with PIPA. They are particularly pleased with some of the innovative features of the Act, such as the protections for personal employee information and for personal information that is disclosed in the course of the sale of a business. At the same time, there is an awareness of the importance of harmonizing privacy legislation.

The Committee recognized that it is particularly important for organizations operating in more than one province to have a consistent approach to private-sector privacy legislation. With this in mind, the Committee reviewed all proposals for amendments to PIPA in the context of the need to maintain similarity with other private-sector privacy legislation.

A review of the federal private-sector privacy Act was under way at the same time as the PIPA review. The House of Commons Standing Committee on Access to Information, Privacy and Ethics issued its recommendations on PIPEDA in May 2007, too late in the PIPA review process to be taken into consideration on every issue. However, Alberta's Select Special Committee considered the recommendations of the House of Commons Committee wherever possible.

The Alberta Committee's final recommendations seek to strike a balance between amending the Act to address the concerns of individuals and organizations and harmonizing Alberta's Act with other privacy legislation.

The Committee believed that the Government of Alberta should continue to monitor amendments to legislation in other jurisdictions with a view to maintaining similarity to other privacy legislation and promoting harmonization. In addition, the Committee called on privacy commissioners and government bodies responsible for private-sector privacy legislation to foster greater understanding of the rights of individuals and the responsibilities of organizations under provincial and federal private-sector privacy legislation.

● Processing personal information outside Canada

The Committee heard that organizations and individuals are concerned that PIPA does not provide adequate protection for personal information transferred to a third party for processing or storage outside Canada.

PIPA expressly states that, where an organization operating in Alberta engages the services of a person, by contract or otherwise, the organization is responsible for that person's compliance with the Act with respect to those services. Organizations continue to be accountable for the security of personal information when it is transferred to a service provider for processing. This is not the case when the service provider is a federally regulated organization subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

PIPEDA applies where personal information is transferred across a provincial border in the course of a commercial activity. PIPEDA expressly requires an organization to use contractual or other means to provide a comparable level of protection while information is being processed by a third party. The Committee heard that the federal Privacy Commissioner has determined that an organization is not obliged under PIPEDA to obtain consent or to provide clients with the ability to “opt out” of having their personal information transferred to a service provider. However, the organization *must* provide *notice* of third-party processing to clients. It is unclear whether the Alberta Information and Privacy Commissioner would follow the federal Commissioner's findings in this matter.

Notice of and consent to transfer personal information outside Canada

PIPA generally requires an organization to obtain consent for the collection, use or disclosure of personal information. When collecting directly from an individual, an organization must provide notification to the individual, before or at the time of collection, of the purpose of the collection and the name of a person who can answer questions about the collection. There is currently no requirement to notify an individual of a transfer of personal information outside Canada.

The Committee considered the increasingly global nature of business, the risks and actual incidents of privacy breaches associated with outsourcing in other jurisdictions, and the differences in the level of protection and disclosure requirements under foreign laws. The Committee also reviewed the requirements for notification and consent and the treatment of outsourcing and contracting under other Canadian privacy legislation.

The Committee believed there was a need to strengthen consumer protection and clarify existing obligations of organizations under PIPA. The Committee understood that requiring notification for third-party processing might require businesses to commit additional resources to their communication processes, but strongly believed that individuals have the right to know that their personal information is being sent outside the country. The Committee unanimously recommended:

1

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.

The Committee also strongly believed that the protection of personal information transferred across international borders by Canadian businesses is a matter that should be addressed at the national level through activities of the federal government and the Privacy Commissioner of Canada. The Committee further recommended:

2

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.

● Notification of a breach of privacy

Privacy breaches can have serious consequences for individuals, ranging from humiliation and anxiety to the use of personal information for criminal purposes, such as fraud. They are matters of great concern to privacy commissioners and the public. A privacy breach can occur even where an organization has systems and procedures in place to protect personal information. PIPA currently does not require organizations to notify individuals that the security of their personal information has been compromised.

Inclusion of a breach notification provision

The Committee considered whether PIPA should be amended to require organizations to notify individuals when their personal information has been compromised, and if so, who should be notified and how a notification provision should be enforced.

The Alberta Information and Privacy Commissioner has issued several rulings on privacy breaches. The Committee considered the recommendations of the Commissioner as well as trends in voluntary notification of affected individuals by Alberta organizations. Members reviewed in detail various matters related to notification, including who should be notified, “triggers” for notification, the risk of harm, “notification fatigue,” the notification format, delays in notification, and the administrative burden on organizations. The broad range of legislative options implemented in other jurisdictions was also considered.

The Committee did not believe that notification should be required in all cases. The Committee thought that organizations should be required to report to the Commissioner breaches that meet certain criteria relating to the risk of harm to affected individuals. The Commissioner could then decide on a case-by-case basis whether notification of affected individuals by organizations was required.

Some Committee members were concerned that delays in notification caused by the Commissioner’s decision-making process could increase the likelihood of harm to individuals. The Committee reasoned that certain types of breaches, such as credit card information loss, will almost always pose an immediate and high risk of harm to affected individuals. Therefore, to mitigate any risk to individuals, the Committee proposed that the Office of the Information and Privacy Commissioner implement a process that would “fast-track” cases in circumstances where notification was time-sensitive.

The Committee unanimously recommended:

3

That the Act be amended to require organizations to notify the Office of the Information and Privacy Commissioner of a privacy breach involving personal information if the privacy breach meets certain criteria, and to notify affected individuals if directed to do so by the Commissioner, subject to the condition that there is an expedited process where notifying the individual is time-critical.

Enforcement of the notification provision

The Committee considered whether it should automatically be a punishable offence for an organization to fail to notify when required to do so, or whether an organization should have an opportunity to rectify its mistake in failing to notify. The Information and Privacy Commissioner can order an organization to perform a duty under the Act; without a new offence provision for the failure to notify, it would be an offence only if an organization ignored a Commissioner's order to notify.

The Committee wanted to ensure that the protection of privacy was the foremost consideration in this matter. With the understanding that prosecution would only be likely in situations where organizations deliberately disregarded the requirement to notify, the Committee unanimously recommended:

4

That the Act be amended to make it an offence not to notify the Office of the Information and Privacy Commissioner of a security breach affecting personal information, where it is reasonable to do so.

◀ Non-profit organizations

PIPA defines a “non-profit organization” as an organization that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or is registered under Part 9 of the *Companies Act*. Non-profit organizations that fall within this definition are required to comply with PIPA only when they collect, use or disclose personal information in connection with a commercial activity. A “commercial activity” is any transaction or conduct that is of a commercial character, and includes the selling or bartering of a membership or donor list and the operation of a private school, a private college, or an early childhood services program.

Other organizations may be not-for-profit in nature but do not fit within the Act’s definition of a “non-profit organization” because, for example, they are established under a private Act of Alberta or under an Act of Canada, or are unincorporated associations. These organizations are fully subject to PIPA, whether or not they carry on a commercial activity.

The Committee considered two issues with respect to organizations in the non-profit sector: whether PIPA should be amended to change the way the Act applies to non-profit organizations, and whether the Act should allow religious organizations to disclose membership lists without the consent of congregation members.

Application of PIPA to non-profit organizations

The Committee was advised that the definition of “non-profit organization” has resulted in different treatment of similar organizations under PIPA (i.e. not-for-profit organizations that fall within the definition and those that do not). This, in turn, has resulted in differences in the way these organizations treat the personal information of their clients, employees, volunteers, and donors.

The Committee heard that some respondents were concerned that requiring all non-profit organizations to comply with PIPA would strain the resources of these organizations and could lead to a decrease in the willingness of individuals to volunteer. The Committee also heard that several other respondents favoured full inclusion under the Act of all non-profit organizations, in order to bring clarity and consistency to the treatment of organizations in the non-profit sector and to ensure the protection of personal information held by these organizations.

The Committee recognized the important role not-for-profit organizations play in the lives of Albertans. The Committee closely reviewed data on the not-for-profit sector in Alberta, which showed the diversity in the services these organizations provide, the populations they serve, the ways in which they are formed, and how many individuals are volunteers or paid staff members. The Committee also examined the way in which the Act protects volunteers from liability.

The Committee considered the types of personal information in the custody or control of organizations in the non-profit sector, as well as the level of protection that this information receives under PIPA compared to the protection afforded under privacy legislation in other jurisdictions. The Committee acknowledged the concern that organizations and other bodies

that are subject to privacy legislation may be reluctant to enter into collaborative programs that require the sharing of personal information with non-profit organizations that are not required by law to protect personal information in their custody (the so-called “chilling effect”). Committee members were particularly concerned that the lack of certainty as to what constitutes a “commercial activity” made it difficult for non-profit organizations to know when they are subject to the Act.

The Committee invited information on the Information and Privacy Commissioner’s experience with non-profit organizations. The Commissioner recommended that all non-profit organizations be covered by PIPA for all their activities, with a one-year transition period to allow the organizations to prepare for compliance.

Committee members favoured an approach that would provide certainty as to who is covered under the Act and would ensure that the privacy rights of an individual are balanced with an organization’s need to collect, use and disclose personal information for reasonable purposes. Committee members agreed that it is important to provide a consistent level of protection for personal information in the custody or control of not-for-profit organizations. The Committee believed that the administrative burden of complying with PIPA could be mitigated by the provision of resources and support to organizations during a one-year transition period.

Recognizing that PIPA was designed to make informational privacy rules easy for small and medium-sized organizations to understand and implement, and that full inclusion of non-profit organizations under PIPA would harmonize Alberta’s Act with that of B.C., the Committee recommended:

5

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

Disclosure of membership lists by religious organizations

The Committee heard that not all churches are treated identically with respect to the ability to disclose a list of members of the congregation to a member to use for matters relating to the affairs of the congregation.

PIPA states that if an Act or regulation authorizes disclosure of personal information, the organization can disclose that personal information without consent. The *Religious Societies’ Land Act* and the *Societies Act* permit disclosure, without consent, of a membership list of the congregation or society (as the case may be) to a member for uses relating to the affairs of that congregation or society. Religious organizations established under other statutes may have to obtain the consent of the members to disclose membership lists.

The Committee noted that some religious organizations do not maintain a membership list; the Committee also found it unclear why obtaining consent would be problematic. Supporting the general principle that there should be limited exceptions to consent, the Committee recommended:

6

That the Act not be amended to add an exception to consent expressly allowing a religious organization to disclose a list of congregation members to a member to use for matters relating to the affairs of the congregation.

● Health information

PIPA was not designed to apply to personal health information. However, PIPA captures certain personal health information that is excluded from the scope of Alberta's *Health Information Act* (HIA) – mainly personal health information related to privately funded health care services. Several responses to the Committee's consultation process expressed concern about the complexity of the legislative framework for the protection of personal health information in Alberta.

The Committee reviewed the legislative framework for the protection of health information; current trends and issues shaping health information legislation, including the program for the electronic health record; and harmonization initiatives.

The Committee appreciated the complexity of the legislative framework for protecting personal health information, the diversity of interests among organizations that collect, use and disclose personal information within and outside the health system, and the effect of differing privacy regimes on organizations and individuals. The Committee considered two issues with respect to health information: the scope of PIPA as it relates to personal health information, and the interaction between PIPA and health information legislation.

Scope of PIPA and the Health Information Act

Committee members considered whether health information that is collected, used or disclosed outside the public health care system should be covered by PIPA or HIA. Currently, personal health information that is collected, used or disclosed by health service providers for the purposes of services provided under extended health benefit plans and other privately funded health services is mostly subject to PIPA.

The Committee examined the application of HIA and PIPA to health information. Particular attention was given to the practical implications of applying the different rules in PIPA and HIA to the collection, use and disclosure of similar personal health information. The Committee understood that a single health service provider who provides services to an individual, but obtains funding from both public and private sources, currently has to comply with both PIPA and HIA.

The Committee was in favour of an approach that would promote consistency in the treatment of personal health information and provide greater clarity and simplicity for organizations collecting, using and disclosing health information, as well as for the public. The Committee recommended:

7

That a recommendation be made to the Minister of Health and Wellness that all personal information about individuals that is collected, used or disclosed for diagnostic, treatment or care purposes be brought within the scope of the *Health Information Act*, regardless of how these health services are funded.

Interaction between PIPA and HIA

The Committee considered whether PIPA or HIA needed to be amended to enhance the interaction between the two Acts. The Committee looked at situations where health service providers subject to HIA (or “custodians”) and organizations subject to PIPA collect personal health information or disclose it to each other in accordance with their respective legislation. This occurs, for example, in a range of relationships between health service providers and organizations that offer health-related products and services.

The Committee considered that, regardless of where the line is drawn as to what health information should be subject to PIPA and what should be subject to HIA, there will continue to be a need for custodians to disclose personal health information to organizations that are not custodians, and for those organizations to collect personal health information from custodians. Where this transfer is for the benefit of the patient and where the patient has given consent for disclosure of personal health information, the legislation should enable the efficient transfer of the information, without multiple requests for the patient’s consent.

The Committee understood that HIA and PIPA do not need to have the same rules with respect to health information, but that custodians and organizations should be able to interact effectively under their respective governing legislation. To ensure that the concerns of organizations are considered when HIA is amended, the Committee recommended:

8

That a recommendation be made to the Minister of Health and Wellness that, in cases where an amendment to the scope of the *Health Information Act* affects organizations currently subject to PIPA, consideration be given to whether it is necessary to authorize personal health information to flow between custodians and organizations.

● Forms of consent

PIPA generally requires an organization to obtain an individual's consent to collect, use or disclose personal information about that individual. The consent requirement ensures that an individual knows that his or her personal information is being collected and the purposes for which the personal information is being collected. PIPA also allows an individual to exercise control over his or her personal information by allowing the individual to put conditions on his or her consent, or to modify or withdraw consent in most circumstances.

The Committee considered two issues concerning consent and the indirect collection of an individual's personal information from an organization or another individual. The first issue was the collection of an individual's personal information from an intermediary organization. The second issue was the collection, use and disclosure of personal information for the purposes of enrolment or coverage in an insurance, benefit or similar plan. The Committee also considered a proposal for a technical amendment relating to the contact information included in a notice for collection.

Indirect collection through an intermediary organization

Strict compliance with PIPA requires each organization involved in a transaction to obtain consent directly from the individual before collecting, using or disclosing personal information for the purposes of that transaction. The Committee heard that this requirement might be a burden for both individuals and organizations in certain circumstances.

It has been a common practice for some organizations to collect an individual's personal information from an intermediary without communicating directly with the individual. This happens, for example, when a health insurance company collects a patient's personal information from a dental practice to process payment for the treatment through an insurance plan. The dental practice acts as an intermediary between the patient and the insurance company.

The Committee looked at real-life scenarios, reviewed related private-sector privacy laws, and examined how different types of consent might affect an individual's knowledge of, and control over, his or her personal information.

The Committee also considered the argument that it is only through the process of directly communicating consent to an organization that many individuals become aware of their ability to control how their personal information is used. Generally, however, Committee members favoured minimizing the burden for individuals and third-party organizations.

The Committee supported an amendment to the Act that would allow an individual to provide consent directly to an intermediary organization to collect the individual's personal information and to disclose that information to a third party for a particular purpose. Under such an amendment, the individual who consented to allow the intermediary organization to disclose his or her personal information to the third party would also be consenting to the third party collecting and using the information for the specified purpose. The Committee understood that the intermediary would provide contact information for the third party to

allow the individual to ask questions about the third party's collection of the individual's personal information.

The Committee reasoned that this approach would be consistent with the operation of the Act in other circumstances, in so far as the individual would have knowledge of, and control over, the way in which his or her personal information was collected, used and disclosed. Recognizing that the amendment would complement current business practices and protect personal information against misuse by third parties, the Committee recommended:

9

That the Act be amended to provide that when an individual consents to the disclosure of personal information by an intermediary for a specified purpose, the individual is deemed to have consented to the collection by the receiving organization for the specified purpose.

Indirect collection for group and family insurance and benefit plans

The Committee heard that it has been a common business practice for insurance companies, when enrolling members in a group or family benefit or insurance plan, to collect the personal information of all members of the plan from a single applicant. For example, an employee usually enrolls his or her family members in an employer benefit plan. A family member may or may not be aware that his or her personal information has been collected or that it will be used for the purpose of the plan.

PIPA generally requires an organization to obtain consent to collect and use an individual's personal information for a specified purpose directly from that individual. An insurance company would have to obtain consent from *each* member of a group or family plan to collect and use his or her personal information for the purpose of the plan.

The Committee agreed that each individual in a plan must have the ability to control how his or her personal information is used. The Committee appreciated that requiring an organization to obtain consent directly from each individual would ensure that each member of the plan had both knowledge of, and control over, how his or her information would be collected and used.

However, the Committee favoured an amendment that would support the longstanding business practice of collecting the personal information of all members of the plan from an applicant. The Committee considered the relationship between the applicant who enrolls members in a plan and the individuals he or she is enrolling and reasoned that, in most cases, the enrolled individual would have knowledge of the benefit plan. In addition, since the insurance company could use the individual's personal information only for the specified purposes, there was little risk that the individual's personal information would be misused by the insurance company.

The Committee reasoned that the individuals enrolled by the applicant could be deemed to have consented to the collection and use of their personal information. This would have the benefit of giving these plan members the ability to withdraw or vary consent. It was noted

that this approach would contribute to harmonization of the Alberta and B.C. Acts with respect to group or family benefit or insurance plans.

The Committee recommended:

10

That the Act be amended to allow an organization to deem an individual to consent to the collection, use and disclosure of his or her personal information for the purpose of coverage or enrolment under an insurance, benefit, or similar plan if the individual has an interest in or derives a benefit from that plan.

Requirements for notification

The Government submission to the Committee proposed a minor amendment to the Act which would allow an organization to provide an individual with *either* the name *or* the position title of a person who can answer an individual's questions about the organization's collection of personal information. PIPA currently requires an organization to notify an individual of the *name* of a person who is able to answer questions about the collection.

The Committee considered the treatment of notification in related Alberta privacy legislation. On the understanding that including the option to provide a position title is likely to make sure that information in a notification remains current, and that this amendment would not diminish an individual's rights under the Act, the Committee unanimously recommended:

11

That the notification provision in the Act be amended to permit an organization to provide an individual with the position title or name of a person who can answer an individual's questions.

● Exceptions to consent

PIPA requires an organization to obtain consent from an individual in order to collect, use or disclose his or her personal information, unless an exception to consent applies.

The Committee considered several substantive issues related to exceptions to consent, including the use of personal information for the purpose of voluntary audits and inspections, and the scope of the existing fraud prevention exception. The Committee also considered whether there was a need to clarify the exclusion for business contact information and the requirement for notification, as well as whether there was a need to continue the Lieutenant Governor in Council's regulation-making powers with respect to exceptions to consent.

The Committee also considered two technical amendments to the Act.

Audits and inspections

The Committee heard that some organizations would like the ability to use personal information without consent to perform voluntary audits and inspections in support of normal business functions.

The PIPA Regulation currently allows an organization to use and disclose personal information without consent for audits and inspections, but only as necessary to comply with an enactment of Alberta or Canada. It is less clear how the Act applies to voluntary audits and inspections.

The Committee considered different types of voluntary audits and inspections performed by organizations, such as performance assessments to improve business processes, environmental impact assessments, and inspections to obtain certification of compliance with international standards. The Committee also considered the collection and retention of personal information by third parties that may perform audits and inspections. Also considered was the relationship between the business purposes of audits and the protections afforded by PIPA's consent requirements.

It was argued that many voluntary audits and inspections could be placed outside the scope of PIPA by anonymizing the information so that it no longer identifies an individual. The Committee recognized, however, that anonymization is not always possible.

Committee members ultimately supported bringing clarity to the Act on this matter. Their main concern was to promote the use of audits and inspections for standard business purposes to the benefit of both organizations and consumers, while protecting against third party misuse of personal information. The Committee recommended:

12

That the Act be amended to allow an organization to use and disclose personal information without consent for the purpose of an audit or inspection of that organization, and to allow an organization performing an audit or inspection to collect, use and disclose personal information for that purpose.

Fraud prevention

PIPA currently permits organizations to collect and disclose personal information without consent for the purpose of preventing, detecting or suppressing fraud, market manipulation, or unfair trading practices. An organization can rely on this exception to consent only if disclosure is by or to an organization that is empowered or recognized under an enactment of Alberta or Canada to carry out fraud prevention activities.

The Government submission proposed two amendments to PIPA's exception to consent for fraud prevention. First, the Government proposed deleting the language that permits an organization to disclose personal information for the purpose of preventing, detecting or suppressing market manipulation and unfair trading practices. This language had become unnecessary as a result of an amendment to the *Securities Act* which added a similar provision to that Act. Second, the Government proposed to clarify that the exception for fraud prevention applies to two national organizations whose ability to carry out fraud prevention investigative activities is not found in legislation.

The Committee considered the history of the exception to consent for fraud prevention, as well as the role of securities, insurance and banking industry organizations in fraud prevention.

Committee members appreciated that the inclusion of a provision for the prevention of market manipulation and unfair trading practices in the *Securities Act* had rendered similar provisions in PIPA redundant. The Committee supported amending the Act to more clearly provide certain organizations with the powers needed to carry out fraud prevention activities. The Committee recommended:

13

That the exception to consent for fraud prevention be amended to delete the current provision for market manipulation and unfair trading practices, and also that the exception be amended to expressly permit the disclosure of personal information by or to designated organizations – namely, the Insurance Bureau of Canada's Investigative Services and the Bank Crime Prevention and Investigation Office of the Canadian Bankers Association – for the purpose of fraud prevention.

Notification for collection of personal information

An organization representing the legal profession suggested to the Committee that PIPA is unclear as to whether an organization that collects information directly from an individual without consent, in circumstances permitted under the Act, must notify the individual even when there is a valid purpose for not informing the individual about the collection.

PIPA requires notification where information is collected directly from an individual. Information may be collected directly from an individual even where consent is not required, as in the case of the collection of a social insurance number by a financial institution to comply with the *Income Tax Act*.

The Committee considered the argument that it might not always be reasonable to require notification in circumstances where the Act permits direct collection of personal information

without an individual's consent. For example, the Act permits an insurance company to conduct surveillance without an individual's consent where there is reason to suspect a fraudulent injury claim. Since the organization is collecting the personal information directly from the individual, PIPA requires that the organization notify the individual of the collection. However, it is likely that notifying the individual in this case would undermine the usefulness of the surveillance.

The Committee considered how the purpose of notification would be served in cases where personal information is collected directly from an individual without consent. The Committee agreed that it was of foremost importance to ensure that an individual has knowledge of how his or her personal information is being collected and used. Committee members thought that it might be reasonable to omit the requirement for notification in some, but certainly not all, circumstances where PIPA permits direct collection of personal information from an individual without consent. To ensure that organizations would be required to give notice where it would be reasonable to do so, the Committee recommended:

14

That the current language of the Act be maintained, which might require an organization to provide notice to an individual when collecting personal information directly from the individual where consent is not required.

Regulation-making powers

PIPA contains provisions allowing the Lieutenant Governor in Council to make regulations adding or expanding upon exceptions to consent for the collection, use and disclosure of personal information. The Government submission proposed deleting these regulation-making powers and moving provisions that are included in the PIPA Regulation into the body of the Act. It was suggested that this measure would promote greater transparency.

The Committee reviewed the historical development of PIPA and the way the regulation-making powers under the Act had been used, as well as alternative processes for amending legislation.

The Committee was reluctant to eliminate the existing regulation-making power since regulations provide a timely way of addressing issues with provisions of the Act, and decided not to pursue this proposal.

Business contact information

The Government submission proposed amending PIPA to clarify that the Act permits disclosure of business contact information to enable persons to contact employees and officials of both private-sector and public-sector bodies. Currently, PIPA does not apply to the collection, use and disclosure of business contact information for the purposes of contacting an individual in his or her capacity as an employee or an official of an organization.

The Committee considered how business contact information is used to facilitate business communications in the private and public sectors and reviewed the intent and current interpretation of the business contact exclusion under PIPA.

The Committee supported extending the provision to encompass employees and officials of public bodies, as well as amending the provision to clearly enable organizations to disclose business contact information in their public communications. The Committee unanimously recommended:

15

That the exclusion for business contact information be amended to clearly enable an individual to be contacted in his or her capacity as an employee, including an official, of either a private-sector or a public-sector body.

Publicly available personal information

PIPA permits the collection, use and disclosure of “publicly available” personal information without consent. The meaning of publicly available is set out in Part 2 of the Regulation under PIPA. The Government submission proposed a technical amendment that would clearly direct users to look at the Regulation to understand the limitations on the collection, use and disclosure of publicly available personal information.

Committee members recognized that users of Alberta’s Act sometimes fail to realize that the scope of publicly available personal information is limited by the Regulation. To promote greater awareness of the restrictions on the collection, use and disclosure of such information, the Committee unanimously recommended:

16

That the Act’s provisions respecting publicly available personal information be amended to include a reference in each case to the meaning of this term that is prescribed in the Regulation.

“Officer of the Legislature”

PIPA does not apply to the collection, use or disclosure of personal information by an officer of the Legislature in relation to the exercise of the officer’s functions under an Act or regulation. The term “officer of the Legislature” is not defined in PIPA. The Government proposed a technical amendment to add a definition of the term “officer of the Legislature” to the Act.

Recognizing that a definition of the term “officer of the Legislature” would clarify the scope of the Act and that a definition of this term exists in the *Freedom of Information and Protection of Privacy Act*, the Committee unanimously recommended:

17

That the Act be amended to add the definition of “officer of the Legislature” that appears in the *Freedom of Information and Protection of Privacy Act*.

● Personal employee information

PIPA defines personal employee information as personal information about an individual who is an employee or potential employee (including a volunteer, apprentice, participant, work experience student, or an individual under contract) that is reasonably required by an organization for the purposes of recruiting an employee or managing or ending an employment relationship with that individual.

The Act permits an organization to collect, use and disclose personal employee information without consent when the information is reasonably required for the employment or volunteer work relationship. In the case of current employees, the organization must give notice that the information is going to be collected, used or disclosed and of the purposes for the collection, use or disclosure.

The Committee considered four issues with respect to personal employee information: the application of the personal employee information provisions in the Act to former employees; how organizations may collect, use and disclose personal information for employment references; whether an official of an organization is an “employee” under PIPA; and the application of the Act’s general “reasonable purpose” requirements to the collection, use and disclosure of personal employee information.

Application of PIPA to former employees

The Committee was advised that inconsistencies in the wording of the personal employee information provisions have given rise to questions about how these provisions apply to former employees. In their submissions to the Committee, the Information and Privacy Commissioner, the Government and some organizations requested clarification on the way PIPA applies to the personal information of former employees.

The Commissioner has determined that the definition of personal employee information refers only to the personal information of *prospective* and *current* employees, but that the disclosure provision for personal employee information applies to *former* employees. The Committee heard that the discrepancies in the provisions meant that an organization could *disclose* employment-related information of former employees for employment-related purposes without consent, but could not *collect* or *use* the personal information of former employees without consent. In addition, former employees would be treated differently from current and prospective employees with respect to fees charged by an organization for responding to an access request for personal employee information.

The Committee considered the nature of the relationship between employers and employees, what information might be considered personal employee information, and how the personal information of employees is treated under other Canadian privacy legislation. The Committee also examined situations where the personal information of former employees might be collected and used for employment-related purposes.

The Committee favoured an amendment that would both protect employees’ privacy interests and support necessary employment-related activities by organizations. Taking the view that

former, current and prospective employees should be treated in the same way under PIPA, the Committee unanimously agreed:

18

That the Act be amended to expand the application of the provisions for “personal employee information” to the personal information of former employees.

Employee references

Several respondents to the Committee’s Discussion Guide suggested that organizations be required to obtain consent to collect, use or disclose an employment reference.

PIPA allows Alberta organizations to *collect* employee references about current or potential employees from other Alberta organizations or public bodies without the consent of the individual the reference is about. The organization is required to give notice to the individual when the individual is a current employee.

There is some inconsistency within the Act with respect to an organization’s ability to give, or disclose, an employment reference without consent. An organization may disclose, without consent, an employee references about a *current* employee, but not about a *former* employee, to another private-sector organization in Alberta. In contrast, an organization can disclose, without consent, employment references about current *and* former employees to a public body.

The Committee considered the discretionary nature of the Act’s provisions for collecting and disclosing references without consent and the Act’s protections for employees’ personal information. The Committee also considered that, in the Information and Privacy Commissioner’s experience, organizations generally obtain consent before collecting or providing employment references for both current and former employees.

Committee members favoured an approach that would provide the highest level of privacy protection for individuals with respect to employment references. The Committee recognized that requiring organizations to obtain consent for collecting and disclosing all employment references might increase the administrative burden for some organizations, but also believed that many organizations were already obtaining consent.

The Committee unanimously recommended:

19

That the Act be amended to require organizations to collect, use and disclose employee references only with the consent of the individual the reference is about.

Definition of an “employee”

The Government submission proposed that the treatment of “officials” be more clearly defined in the Act. The Committee heard that the definition of “employee” in the Act was intended to include all individuals providing services for or on behalf of an organization. However, PIPA’s exclusion for business contact information distinguishes between

employees and officials, and PIPA’s definition of an employee does not include officials. An organization might, therefore, argue that an official cannot be an employee.

The Committee reviewed all the provisions in PIPA that specifically apply to employees, including the provisions for personal employee information, business contact information, “whistleblower” protection, and fees for processing a request for personal employee information.

The Committee considered that the change in the definition of “employee” to include an “official” would have minimal impact on not-for-profit organizations. Officials of not-for-profit organizations that must comply with the Act are likely already included within the definition of “employee” as volunteers or employees.

Committee members agreed that officials should have the same rights and protections as employees under PIPA. The Committee recommended:

20

That the definition of “employee” be amended to clarify that all provisions of the Act that apply to “employees” of an organization also apply to officials of an organization, and that the provision for business contact information be simplified to refer to “an employee of an organization.”

Limitations on the collection, use and disclosure of personal information

The submissions of the Government and the Information and Privacy Commissioner proposed that the Act be amended to clarify that the “reasonable purpose” principles apply to the collection, use and disclosure of personal employee information, as well as personal information related to the sale or purchase of a business.

PIPA’s provisions for the collection, use and disclosure of personal information begin with two general principles: that an organization may collect, use or disclose personal information *only for purposes that are reasonable and only to the extent that is reasonable for those purposes*. It was reported that the question has arisen whether the reasonable purpose requirement applies to the collection, use and disclosure of personal employee information and to personal information that an organization wants to collect, use or disclose for the purpose of selling or acquiring a business.

The Committee considered that PIPA’s purpose is to protect personal information in a manner that recognizes the rights of the individual and the need of organizations to collect, use and disclose personal information *for purposes that are reasonable*.

To ensure that a “reasonableness” test will be applied in support of the Act’s purpose in all circumstances, the Committee recommended:

21

That the language of the provisions for collection, use and disclosure of personal information without consent be amended to clarify that an organization may collect, use or disclose personal information, including personal employee information, only for purposes that are reasonable and only to the extent that is reasonable for those purposes.

● Access to records containing personal information

PIPA permits individuals to make an access request to an organization for their own personal information. The right of access, which applies only to recorded personal information, requires an individual to make a written request to the organization that he or she believes has the record.

The Act permits, and sometimes requires, an organization to withhold certain information in the requested record. The process for responding to an access request, including time limits, is set out in the Act. If access is refused, the individual must be given reasons for the refusal, as well as contact information for a person who can answer questions about the refusal. The individual has the right to request a review by the Information and Privacy Commissioner of the organization's decision.

The Committee heard that the access process under the Act was generally thought to be working well. The Committee considered recommendations with respect to continuing requests and the failure of an organization to respond to access requests. The Committee gave particular attention to the question of "work product information" and whether to explicitly exclude from the right of access information in a record prepared or collected by an individual in his or her capacity as an employee.

Continuing requests

The Committee considered a proposal to add a provision for continuing requests. A continuing (or "standing") request allows an individual to receive information at regular intervals.

PIPA does not allow for continuing requests. The Committee reviewed situations where an individual might like to have regular updates on his or her personal information. The Committee also considered how a continuing request process might work, including costs to users and administrative requirements of the process.

The Committee determined that an individual could use existing processes to obtain periodic updates of their personal information, and decided to make no recommendation on continuing requests at this time.

Work product information

An individual may produce and collect many types of records, including reports, correspondence and memoranda, as part of his or her employment responsibilities. This is often referred to as "work product information." This information is usually not about the individual who produced or collected the information. PIPA does not expressly exclude work product information from the definition of personal information or from the scope of the Act.

The Committee considered the way in which organizations and the Information and Privacy Commissioner might apply the Act to work product information. First, a determination would be made as to whether the information produced or collected by the employee is about the employee. If the information is *about* the individual, it would be personal information and

subject to access under PIPA; if it is *not about* that person, it would not be subject to the Act and there would be no right of access to it under the Act.

This approach recognizes that there are instances where information produced by an employee might be personal information, depending on the context in which it is being used. For example, an employee might request a piece of correspondence he prepared in the course of employment which resides in the organization's operational files. This would most likely be considered work product information. However, if the same piece of correspondence were used in a performance appraisal to determine the employee's skills or knowledge, the information might be considered personal information about the employee; this would mean it was personal information under the Act.

Reasoning that the current contextual approach allows for greater flexibility than a categorical exclusion, the Committee recommended:

22

That the definition of "personal information" remain unchanged, with no reference to "work product information," so as to continue to allow an organization to consider the context when deciding whether information in a record created as part of an individual's employment responsibilities is "personal information."

Failure of an organization to respond to an access request

The Government submission to the Committee proposed an amendment to the Act that would deem an organization's failure to respond to an access request to be a refusal of a request for access.

PIPA allows an applicant to challenge a decision made by an organization under the Act within 30 days of being notified of the decision. PIPA does not provide any direction on how this time limit is applied when an organization fails to act upon a request as required under the Act.

With the understanding that an individual's request must be refused in order for the individual to request a review, and that an organization that fails to respond can apply for an extension of time when needed, the Committee unanimously recommended:

23

That the Act be amended to include a provision allowing for deemed refusal of a request for access if an organization refuses to respond to the request, so as to allow the individual a right to request a review.

❶ Exceptions to access

An individual's right of access under PIPA is subject to limited and specific exceptions set out in the Act. These exceptions to access may *permit* the organization to decide whether to disclose the information (as in the case of information that was collected for an investigation) or may *require* an organization to refuse access (as in the case of personal information about another individual).

The Committee heard that respondents to the Discussion Guide had a few concerns about existing exceptions to access, and the Committee considered two of these in detail. The first issue was whether the exception for confidential information of a commercial nature should be more clearly defined to include personal information in corporate succession, redundancy and restructuring plans. The second was whether there should be an exception for information in a record subject to a solicitor's lien.

Confidential information of a commercial nature

The Committee considered the appropriate balance between an employee's right of access to personal information about his or her future employment relationship with an organization and the organization's ability to protect confidential information related to corporate succession, redundancy or restructuring plans.

There is currently an exception to access in PIPA which gives organizations the ability to decide whether to disclose "information of a commercial nature." The Act does not define information of a commercial nature. It is unclear whether corporate succession, redundancy or restructuring plans would fall within this exception. The treatment of personal information in plans of this kind has not been addressed by Canadian privacy commissioners.

Taking into consideration the general satisfaction with the present access provisions, the advantages of continuing consistency with other Canadian jurisdictions and the likelihood that the scope of the exception will be clarified through rulings of the Information and Privacy Commissioner, the Committee unanimously recommended:

24

That the exception for confidential information of a commercial nature not be amended at this time, allowing the matter of access to personal information in a succession, redundancy or restructuring plan to be addressed through the independent review process.

Records subject to a solicitor's lien

Two organizations representing the legal profession brought to the attention of the Committee that PIPA could interfere with an existing legal right to withhold personal information subject to a solicitor's lien. A solicitor's lien allows a lawyer to maintain possession of, and refuse access to, a client's file until all charges and fees owed for services rendered have been paid.

An organization cannot currently refuse an individual access to his or her personal information under PIPA on the basis that the information is in a record that is subject to a

solicitor's lien. It was noted that the Information and Privacy Commissioner supported an amendment to PIPA authorizing an organization to refuse access to information in a record that is subject to a solicitor's lien.

The Committee considered existing exceptions to access for personal information of third parties and other exceptions that might apply to information held in a lawyer's file. The Committee also considered the Commissioner's powers with respect to access and fees, and the fact that there is a legal process whereby clients can have legal fees reduced or disallowed. Concerns were expressed that the addition of an exception for a solicitor's lien might result in other professions requesting similar exceptions to allow personal information to be withheld against unpaid accounts.

The Committee unanimously recommended:

25

That the Act not be amended to add an express exception to access for personal information in a record that is subject to a solicitor's lien.

◀ Fees

An organization may charge an individual a reasonable fee for access to records under PIPA. “Reasonable” means what a reasonable person would consider appropriate in the circumstances. The Act establishes certain rules respecting fees, such as requiring an organization to provide an estimate before processing a request, but the Act does not set fees for particular services. An individual who believes that a fee is not reasonable may request that the Information and Privacy Commissioner review the fee charged by an organization. An organization may not charge a fee to process a request from an employee for access to his or her own personal employee information.

The Committee heard that most respondents considered the Act’s provisions relating to fees appropriate. The most significant issue was whether the Act should prescribe the maximum fees an organization may charge in response to an access request. The Committee also considered some technical matters relating to fees.

Fee schedule

The Committee heard that both applicants and organizations are sometimes unsure what might be a reasonable fee for an organization to charge for the processing of an access request. Several respondents suggested that a fee schedule might remove this uncertainty.

The Committee considered the process of determining fees under PIPA, fee provisions in related laws, the actual cost of processing access requests, the use and purpose of fee schedules in public-sector access-to-information legislation, and existing guidance on fees in the private sector. The Committee also considered the individual’s right to challenge an unreasonable fee through the review process, and the Commissioner’s experience in reviewing fees for processing access requests.

Reasoning that few individuals to date had requested a review of fees and with the understanding that many organizations do not charge fees for access to records, the Committee decided not to make a recommendation regarding the creation of a fee schedule under PIPA at this time.

Waiver of fees

A technical amendment was proposed by the Government to resolve an inconsistency in the Act regarding the waiver of fees by organizations. PIPA does not include a provision requiring an organization to consider a request by an individual to excuse a payment of fees. Nevertheless, there is a reference in the Act to excusing payment of fees in a provision relating to time limits for responding to access requests.

With the understanding that the removal of this reference to excuse payment would not take away an organization's ability to waive a fee if it should choose to do so, and to promote consistency within the Act, the Committee unanimously recommended:

26

That the reference to excusing payment of a fee be deleted from the Act's provisions respecting time limits for requesting a review, since the Act does not require an organization to consider a request to excuse payment of a fee.

Fees for correcting personal information

The Government submission to the Committee drew attention to a possible source of uncertainty in the Act regarding fees. PIPA does not allow an organization to charge a fee for the correction of personal information unless otherwise specified in the regulations. However, no such regulation currently exists and none is contemplated. A technical amendment was proposed to remove any uncertainty on this matter.

Since there was no suggestion that there should be any exception to the rule that an organization cannot charge a fee for making a correction, the Committee unanimously recommended:

27

That the phrase "subject to the regulations" be deleted from the Act's provisions respecting fees for the correction of personal information, since regulations on this matter are not contemplated.

Professional regulatory organizations

Professional regulatory organizations (PROs) are generally self-governing professional or occupational bodies incorporated under a statute that provides for membership in, and the regulation of, that profession or occupation. These bodies regulate the standards of education and experience required of members to enter the profession or occupation, their standards of practice, continuing education requirements, and the conduct of members. PROs also investigate and adjudicate complaints from the public or other members about alleged unprofessional conduct.

Alberta has fifty-five PROs, twenty-seven of which are outside the health field. Examples of PROs include the Law Society of Alberta, the College of Physicians and Surgeons of Alberta, and the Real Estate Council of Alberta, as well as occupational associations, such as the Association of School Business Officials of Alberta.

Personal information codes

PIPA allows PROs the option of either following PIPA's provisions with respect to the collection, use and disclosure of personal information, or developing a personal information code that is "consistent with the purposes and intent" of the Act. Personal information codes are intended to allow PROs to present a simplified version of the principles set out in the Act that is directly relevant and meaningful to the profession, its members and the public. The Committee heard that there are currently no personal information codes in place for PROs.

Several professional regulatory organizations suggested to the Committee that the provisions for "personal information codes" in PIPA do not address their concerns regarding compliance with both their own governing legislation and separate privacy legislation.

The Committee reviewed the role of PROs in Alberta, how PIPA and other Canadian privacy legislation apply to PROs, types of personal information held by PROs, and the advantages and disadvantages of developing a personal information code within a professional regulatory organization.

Although some PROs expressed interest in retaining the code provisions if a code could be more responsive to the needs of PROs, these organizations did not provide the Committee with details on how the provisions might be developed to address their concerns. It was unclear how the code provisions in PIPA could be amended to respond to the concerns of PROs while ensuring that a code provides the same level of privacy protection as the Act.

Committee members favoured maintaining the present ability of PROs to address their concerns in a manner that does not affect other organizations subject to PIPA. Recognizing that it may be premature to decide that PROs might not benefit from the flexibility offered by the power to establish a personal information code, the Committee recommended:

28

That the provisions for personal information codes be maintained and the issue of modifying or deleting these provisions be revisited during the next review of PIPA.

◀ Managing personal information

PIPA is not intended to govern records management generally within organizations. Nevertheless, PIPA does require organizations to develop and follow policies and practices that are reasonable to meet their obligations under the Act. PIPA recognizes that there is a direct link between the protection of personal information and the management of records containing personal information.

Several respondents raised concerns with respect to the management of personal information by private-sector organizations. The Committee gave particular attention to proposals relating to the retention and accuracy of personal information.

Retention of personal information

PIPA states that an organization may retain personal information for as long as is reasonable for legal or business purposes. The Act provides no specific guidance as to what retention periods are considered reasonable.

With one specific exception, the PIPA does not require organizations to anonymize, de-identify, or destroy information when it is no longer required for legal or business purposes. The exception is that the Information and Privacy Commissioner may order an organization to destroy personal information that has been collected in circumstances that are not in compliance with the Act. It is not clear that the Commissioner could order an organization to destroy personal information that was no longer needed for legal or business purposes.

In his submission, the Commissioner suggested that the Act should expressly limit the retention of personal information that is no longer required for legal or business purposes. This would reduce the risk of improper use by the organization and limit the risk of a security breach.

The Committee supported an approach that would require organizations to dispose of personal information that is no longer needed. Committee members recognized the importance of ensuring that records that are no longer required are effectively destroyed. In addition, the Committee believed that the Commissioner should have the ability to enforce the proper disposal of information, subject to the reasonableness standard that applies throughout the Act. With the understanding that such an amendment would more closely align Alberta's approach to records destruction and anonymization with that of B.C. PIPA, and provide enhanced protection of personal information in the custody of organizations, the Committee recommended:

29

That the Act be amended to require an organization to destroy or anonymize, within a reasonable time, personal information that an organization no longer requires for legal or business purposes, and to add a definition of destruction to the Act.

Retention period for records relating to a Commissioner's investigation

The Information and Privacy Commissioner proposed that PIPA be amended to require organizations to retain records relating to an investigation by the Commissioner for at least one year from the conclusion of the investigation.

Since PIPA currently allows organizations to retain personal information for as long as is reasonable for legal or business purposes, an organization could certainly retain records that could be required if a complainant requested a review by the Commissioner or applied for a judicial review of a decision by the Commissioner.

There were some concerns about specifying a specific retention period for specific classes of records, primarily because this could have implications for the retention of other classes of records.

Ultimately, the Committee favoured establishing a retention period of one year. Not only would this provide clarity for organizations, the one-year retention period would ensure that an individual had a right of access to personal information in the records. The Committee recommended:

30

That the Act be amended to require an organization to retain records relating to an investigation by the Commissioner for at least one year after the conclusion of an investigation.

Accuracy of personal information

PIPA requires an organization to make a reasonable effort to ensure that personal information it collects, uses, or discloses is “accurate and complete.” There are currently no limits on how frequently or for what purposes information may be maintained or updated.

The Government submission proposed an amendment to the Act which would limit the requirement to ensure accuracy and completeness to what is reasonable for the purposes for which the organization will use the information.

The Committee considered limitations on the requirement to ensure accuracy and completeness in both B.C. PIPA and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The limitations in both Acts discourage organizations from maintaining and updating personal information unnecessarily, to protect against misuse of personal information by organizations.

To promote increased protection of personal information and harmonize Alberta's Act with the B.C. and the federal legislation on this matter, the Committee recommended:

31

That the provision requiring an organization to ensure the accuracy and completeness of personal information be amended to state that an organization must ensure that personal information is accurate and complete to the extent that is reasonable for the organization's purpose in collecting, using or disclosing the information.

◀ The independent review

PIPA provides for independent oversight by Alberta's Information and Privacy Commissioner. The Commissioner also oversees the *Freedom of Information and Protection of Privacy Act* and the *Health Information Act*.

The Commissioner has the power to investigate a complaint about an organization or to review a decision made by an organization regarding a request for access to an individual's own personal information. If a matter is not settled through mediation or investigation, the Commissioner can hold an inquiry and issue an order. The Commissioner can also direct an individual to pursue another complaint resolution procedure before the Commissioner will deal with the complaint.

The Committee heard that respondents to the Discussion Guide were divided as to whether the processes established by the Act for the Commissioner to conduct investigations and to review decisions of organizations are appropriate. There were many different proposals for changes to the Commissioner's processes and powers. The Committee reviewed proposals from the public, as well as recommendations from the Commissioner, relating to complaint processes, the Commissioner's power to compel the production of records subject to solicitor–client privilege, restrictions on disclosure of information by the Commissioner, time limits for investigations and reviews, the ability to conduct audits and enter premises, the Commissioner as a compellable witness, orders following inquiries, and the judicial review process. The Committee also considered two technical matters relating to the Commissioner's powers.

Early dismissal of complaints and requests for review

The Committee heard that organizations are concerned that in some cases resources are being expended on investigations and inquiries that are unlikely to lead to effective resolution. There were several proposals for amendments to PIPA to allow for early dismissal of unsupported complaints. PIPA currently allows organizations to apply to the Information and Privacy Commissioner for authorization to disregard an *access request* on the grounds that it is frivolous or vexatious.

The Committee focused on two recommendations made by the Commissioner that would allow for the early dismissal of complaints that are clearly without merit.

The first proposed amendment would authorize the Commissioner to discontinue investigations or reviews when the Commissioner believes the complaint or request for review is without merit or where there is not sufficient evidence to proceed. The second proposed amendment would permit an organization to apply to the Commissioner for authorization to disregard a frivolous or vexatious *complaint*.

The Committee considered the Commissioner's powers and processes for investigations and reviews. Particular attention was paid to protecting the right of an individual to complain or request a review; the costs involved in inquiries; the Commissioner's experience with complaints that were found to be without merit, frivolous or vexatious; and the treatment of

such complaints in other Canadian privacy legislation and in other Alberta statutes. The Committee agreed that a balance must be maintained between an individual's right to complain or request a review and an organization's ability to operate without the burden of frivolous or vexatious complaints.

The Committee believed that the Commissioner should be given an express power to dismiss unsupported complaints early in the complaint process. With the understanding that such an amendment would not lessen an individual's right to have a complaint investigated and resolved under the Act, and would promote more effective use of resources within the Commissioner's Office and within organizations, the Committee recommended:

32

That the Act be amended to provide the Commissioner with explicit authority to discontinue an investigation or a review when the Commissioner believes the complaint or request for review is without merit or where there is not sufficient evidence to proceed.

The Committee was of the view that this authority to discontinue an investigation into a complaint without merit would also allow the Commissioner to discontinue an investigation into a complaint where the organization satisfied the Commissioner that the complaint was frivolous or vexatious. The Committee therefore decided not to recommend amending the Act to permit an organization to apply to the Commissioner for authorization to disregard a frivolous or vexatious complaint.

Solicitor–client privilege

The Information and Privacy Commissioner's submission to the Committee proposed that the Act be amended to explicitly state that the Commissioner can compel the production of documents that are subject to solicitor–client privilege, without affecting that privilege.

Currently, PIPA states that when conducting an investigation or inquiry, the Commissioner can require an organization to produce records for the Commissioner, notwithstanding any privilege of the law of evidence. The phrase "any privilege of the law of evidence" is found in many other privacy statutes in both the public and private sector, and has generally been accepted as including solicitor–client privilege. However, this interpretation is now uncertain, as a result of recent court decisions on solicitor–client privilege.

The Committee heard that some organizations argue that the Commissioner is not authorized to examine documents in cases where organizations claim solicitor–client privilege. The Committee appreciated that, without the ability to examine the records, the Commissioner cannot provide a complete review of an organization's response to an access request.

The Supreme Court of Canada is expected to consider the matter of solicitor–client privilege in a case that is scheduled for early 2008. The case concerns the power of the federal Privacy Commissioner to compel documents under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Committee decided that a legislative amendment regarding solicitor–client privilege should take into account any guidance offered by the

Court. The Committee therefore decided not to recommend providing the Commissioner with the power to compel documents subject to solicitor–client privilege at this time.

No waiver of privilege

When information that is subject to solicitor–client privilege is disclosed to third parties, the privilege is normally waived. This means that the information is no longer protected by the privilege in any context.

The Information and Privacy Commissioner’s submission proposed that the Act be amended to expressly state that, when information that is subject to solicitor–client privilege is disclosed to the Commissioner at the Commissioner’s request, the privilege is not waived.

The Committee understood that, under the current provisions of the Act, solicitor–client privilege will likely not be waived if documents subject to that privilege are disclosed to the Commissioner as required under the Act. However, recognizing that the proposed amendment would create certainty for organizations concerning the protection of solicitor–client privilege, the Committee recommended:

33

That the Act be amended to state that when information to which solicitor–client privilege applies is disclosed to the Commissioner at his request, this solicitor–client privilege is not affected.

Disclosure of evidence of an offence to the Minister of Justice and Attorney General

PIPA does not give the Information and Privacy Commissioner the power to determine whether an offence under PIPA was committed, or to levy fines for committing an offence under PIPA. An offence under PIPA must be referred to the Minister of Justice and Attorney General for prosecution in the Alberta courts.

There has been concern that the Commissioner may not be able to disclose information to the Attorney General to initiate a possible prosecution. PIPA states that the Commissioner cannot disclose information obtained during an investigation or inquiry under PIPA, except in specified circumstances. The Commissioner can, for example, disclose information in an investigation report or an order, but the disclosure must be limited to what is necessary for the purposes of establishing the grounds for recommendations or orders. Restrictions such as these may make it difficult for the Commissioner to bring a possible offence to the attention of the Attorney General.

The Commissioner and the Government proposed that the Act be amended to allow the Commissioner to disclose to the Attorney General information relating to the commission of an offence under an enactment of Alberta or Canada if the Commissioner considers there is evidence of a possible offence.

The Committee considered restrictions on disclosure of information in public- and private-sector privacy legislation in Canada, noting that Alberta’s *Freedom of Information and*

Protection of Privacy Act (FOIP Act) and both the B.C. and federal private-sector privacy Acts permit disclosure for the purpose of advising the Attorney General of a possible offence.

The Committee appreciated that the Commissioner and his staff have access to a wide range of information, including information that is not subject to PIPA. The Committee also appreciated that the Commissioner has exercised the power to disclose information to the Attorney General under the FOIP Act only in cases where the Commissioner was satisfied there was clear evidence of a possible offence.

Committee members heard that a power to disclose information to the Attorney General would be a significant exception to the general restrictions on disclosure, but agreed that allowing for disclosure of information of an offence would support the administration of justice. However, to protect the interests of parties involved in investigations and inquiries performed under the Act, the Committee agreed that the provision should prohibit the Commissioner from disclosing evidence contained in a privileged record.

The Committee recommended:

34

That a provision be added to the Act to allow the Commissioner to disclose to the Minister of Justice and Attorney General information relating to the commission of an offence under an enactment of Alberta or Canada if the Commissioner considers there is evidence of an offence, subject to the condition that the Commissioner must not disclose information that is subject to solicitor–client privilege.

Time limits for inquiries

PIPA states that an inquiry arising from a request for a review or complaint must be completed within 90 days from the day a written request or complaint is received by the Information and Privacy Commissioner, unless the Commissioner provides written notification of an extension and an anticipated date for the completion of the review.

The Committee heard that, until recently, the existing 90-day time limit has been interpreted as a flexible target rather than a mandatory deadline. However, a July 2007 decision of the Court of Queen’s Bench stated that 90 days is a mandatory deadline for completing an inquiry, unless an extension is in effect. As a result of this decision, if an inquiry is not completed within 90 days, or a longer time period set by the Commissioner, the Commissioner loses jurisdiction in the matter. The Commissioner proposed that the Act’s provision for a 90-day time limit be repealed or that the time limit be extended from 90 days to two years (with no change in the Commissioner’s power to extend the time limit).

The Committee considered the Office of the Information and Privacy Commissioner’s process and experience in addressing complaints and conducting reviews and inquiries. Committee members requested statistics on completion rates, and invited comments on scheduling, resources, and administrative requirements for all parties involved in these processes. Committee members reviewed the 2007 decision, and also heard about the challenges facing the Office of the Information and Privacy Commissioner in estimating

completion times. They considered the effect of deadlines on the rights of individuals under PIPA, as well as time limits in access and privacy laws in other jurisdictions and for other Alberta tribunals.

Committee members were in favour of a time limit to promote accountability in the review, complaint and inquiry processes, and to protect the rights of individuals under the Act. It was agreed that one year was an appropriate time limit. The Committee recommended:

35

That the Act be amended to provide that all processes relating to a complaint or request for review must be completed within one year of receiving the complaint or request for review where practicable, with the Commissioner retaining the ability to extend timelines where necessary.

Audit powers

The Information and Privacy Commissioner is empowered to conduct investigations and inquiries under the Act. Following an inquiry, the Commissioner can order an organization to perform a particular action or discontinue a particular practice.

In his submission to the Committee, the Commissioner proposed an amendment to the Act to empower the Commissioner to initiate an audit of an organization. The Committee understood that an audit power would enable the Commissioner to determine whether an organization has complied with an order following an inquiry. An audit power would also enable the Commissioner to assess an organization's general compliance with PIPA, if the organization's activities warranted an audit.

The Committee supported processes for monitoring compliance with the Act that allow the Commissioner to educate organizations without penalizing non-compliance. Recognizing that the Commissioner currently has the ability to provide advice and recommendations to organizations, and to conduct investigations that do not result in orders against the organization, the Committee decided that it was not necessary at this time to amend the Act to provide the Commissioner with the power to initiate an audit of an organization.

Power to enter premises

In the course of an investigation or inquiry, the Information and Privacy Commissioner can compel the production of records and examine those records, regardless of whether the records are subject to the Act. The Commissioner does not currently have the ability to enter an organization's premises during an investigation or inquiry, unless given permission by the organization.

The Committee heard that the nature of some investigations conducted by the Commissioner or his staff require visits to the organization's premises. However, the Committee also heard that many organizations have voluntarily allowed the Commissioner and his staff to enter their premises during investigations and inquiries. The Committee decided not to make a recommendation to provide the Commissioner with the power to enter premises during an investigation or inquiry.

Commissioner as a compellable witness

The Information and Privacy Commissioner's submission to the Committee proposed an amendment to the Act that would expressly state that neither the Commissioner nor anyone acting under his direction can be compelled to give evidence in a court or in other proceedings.

The Act restricts the disclosure of information obtained by the Commissioner and his staff during the performance of their duties. The Act also limits the admissibility of statements made by a person during an investigation or inquiry by the Commissioner as evidence in other proceedings.

The Committee heard that the restrictions on the disclosure of information under PIPA are intended to preserve the confidentiality of investigations and proceedings before the Commissioner. The Committee also heard that it was not clear whether the existing restrictions are sufficient to keep the Commissioner and his staff from being compelled to give evidence in other proceedings. The Committee considered that an amendment to PIPA would bring greater certainty to the Act and would be consistent with legislation in other jurisdictions.

The Committee recommended:

36

That the Act be amended to explicitly state that neither the Commissioner nor anyone acting on his behalf or under his direction can be compelled to give evidence in a court or in any other proceedings, except as specified in the Act.

Judicial review process

The Act requires the Information and Privacy Commissioner to issue an order upon completing an inquiry. A person can apply to the Court of Queen's Bench for judicial review of the Commissioner's order within 45 days of receiving the order.

If an application for judicial review is made, the Commissioner's order is stayed (i.e. suspended) until the court has dealt with the matter. The court can extend the 45-day time limit for applying for judicial review. The request for an extension can be made before or after the 45-day period has expired.

In his submission to the Committee, the Commissioner proposed that the statutory stay of a Commissioner's order pending determination of the application for judicial review be deleted from the Act. The Commissioner also proposed removing the power of the court to extend the 45-day time limit for bringing an application for judicial review.

The Committee heard that an application for judicial review may be commenced but not heard by the court for various reasons. When this occurs, the Commissioner's order is stayed indefinitely, with the result that the organization does not have to comply with it. The Committee also heard that the ability of the court to extend the time for applying for judicial review creates uncertainty regarding the time limit for an organization to comply with a Commissioner's order.

The Committee believed it is important that a person have an opportunity to ask the court to review a decision of the Commissioner. However, the Committee was concerned about the length of time that a Commissioner's order could be without effect as a result of the time lines for the judicial review process. The Committee noted that an organization might use the judicial review process to delay or avoid compliance with a Commissioner's order. The Committee considered that any abuse of the system could be minimized by a shorter time period for applying for judicial review, with no possibility of extension and no legislated stay of the order.

The Committee unanimously recommended:

37

That the Act be amended to delete the provision with respect to staying a Commissioner's order such that an organization must comply with an order of the Commissioner.

The Committee further recommended:

38

That the Act be amended to provide that an application to a court for judicial review of a Commissioner's order must be made within 5 business days from the day that the person making an application is given a copy of the order.

Duty to make an order

The Government submission proposed an amendment to the Act that would allow the Information and Privacy Commissioner to not issue an order on a matter of inquiry related to access to personal information where none of the options for orders is applicable.

PIPA states that when the Commissioner hears an inquiry, the Commissioner *must* dispose of a matter relating to access to personal information by making an order. The order must direct an organization to give or refuse access, confirm a decision made by an organization, or require an organization to reconsider its decision.

The Committee considered circumstances under which the options for orders might not be applicable. The Committee also considered the relationship between the issuing of an order and the right to apply for review of a Commissioner's decision.

The Committee was concerned that removing the requirement for an order might affect an individual's ability to pursue damages for breach. Ultimately, however, the Committee recognized that there were circumstances where an order would be meaningless, such as where the records at issue in an inquiry have been disclosed to the applicant during the inquiry process. To provide flexibility to the Commissioner where necessary, the Committee recommended:

39

That the provision for orders that may be issued after inquiry be amended to allow the Commissioner not to issue an order, so as to remove the necessity of an order on a matter where none of the options for orders is applicable under the circumstances.

Access to recorded personal information

A technical amendment to the Act was proposed by the Government to ensure that all provisions in the Act with respect to access requests refer to a request for *recorded* personal information.

The Information and Privacy Commissioner has the power to hold an inquiry and make an order respecting an organization's decision to give or refuse access to an individual's "personal information." However, other provisions of the Act that refer to access requests make it clear that the right of access is limited to *recorded* personal information.

The Committee agreed that this inconsistency in the language of the Act requires correction, and recommended:

40

That the provisions referring to the Commissioner's powers to hold inquiries and make orders relating to access requests be amended, for consistency, to refer to requests for recorded personal information.

Notification of a review or complaint

The Government submission proposed to amend the Act to use consistent terminology with respect to the provision of copies of requests for reviews or complaints.

When a person makes a request for a review or to initiate a complaint, the Information and Privacy Commissioner must give a copy of the request to the organization concerned and "any other person that the Commissioner considers appropriate." Another provision of the Act however, refers to giving a copy of a request to "a person affected by the request."

To address this inconsistent use of language and provide further clarification on the Commissioner's powers and who may receive a copy of a request, the Committee recommended:

41

That the provision for severing a request for review or complaint before providing it to other persons be amended to refer to the organization concerned and any other person *that will receive a copy of the request*.

● Offences and penalties

The aim of penalties for regulatory offences is to protect the public from the risk of social harm and promote compliance with the regulatory framework. PIPA creates six regulatory offences for specific contraventions of the Act. Offences under PIPA are prosecuted by the Crown. PIPA permits the courts to impose a fine on a person found guilty of an offence under the Act. The Act also includes a defence of reasonable care.

A few respondents to the Discussion Guide suggested changes to the offence and penalty provisions in the Act. The Information and Privacy Commissioner also proposed several changes to these provisions. The Committee gave particular attention to proposals to create offences for failing to safeguard personal information, for contravening PIPA's "whistleblower" protection provisions, and for destroying evidentiary records. The Committee also considered the standard of proof for offences, the limitation period for prosecutions under the Act, and penalties.

Failure to make reasonable security arrangements

If an organization fails to make reasonable security arrangements to protect personal information in its custody or control, the Information and Privacy Commissioner can conduct an inquiry and order the organization to implement necessary security measures.

However, the organization cannot be prosecuted for an offence under the Act unless it fails to follow the Commissioner's order to make reasonable security arrangements. This essentially gives an organization a "second chance" to comply with the duty to make reasonable security arrangements before it can be prosecuted for a contravention of the Act. The Commissioner suggested in his submission to the Committee that PIPA be amended to create a new offence for the failure to make reasonable security arrangements; this would essentially eliminate the "second chance."

While supporting an expectation of compliance with the Act, the Committee understood that an organization currently risks prosecution for an offence under the Act if it does not comply with a Commissioner's order to make reasonable security arrangements to protect personal information. Taking the view that the creation of an offence for the failure to make reasonable security arrangements would be onerous for organizations, especially in the not-for-profit sector, the Committee favoured maintaining the existing requirements in the Act for safeguarding personal information.

Contravention of "whistleblower" protections

PIPA states that an organization cannot take adverse employment action against an employee or deny an employee a benefit for reporting a contravention of the Act to the Information and Privacy Commissioner, for refusing to do something that would contravene the Act, or taking an action that would avoid a contravention of the Act. These are PIPA's "whistleblower" protection provisions.

The Commissioner suggested in his submission that PIPA be amended to make it an offence to contravene these whistleblower protection provisions. The Committee understood that, while the Commissioner can currently order an organization to cease taking adverse action against an employee, the organization could only be prosecuted for an offence if it ignored this order.

The Committee noted that, with the exception of Alberta's PIPA, all the privacy statutes in Canada that contain whistleblower protection provisions also contain an offence provision for contravening these protections. The Committee recommended:

42

That the Act be amended to make it an offence to contravene the “whistleblower” protection provisions under the Act.

Destruction, alteration, falsification, or concealment of evidentiary records

It is currently an offence under PIPA to obstruct the Information and Privacy Commissioner in the course of the performance of his duties under the Act. In his submission, the Commissioner suggested an amendment to the Act to create a specific offence for the destruction, alteration, falsification, or concealment of evidentiary records during an investigation or inquiry by the Commissioner.

The Committee was advised that the existing offence in the Act for obstructing the Commissioner may already prohibit an organization from destroying, altering, falsifying, or concealing evidentiary records during an investigation or inquiry. However, the Committee was concerned that some organizations may not understand that they must not dispose of any evidentiary records once notified of an investigation or inquiry. Reasoning that a new offence would create certainty on this point, the Committee recommended:

43

That the Act be amended to make it an offence for a person to dispose of, alter, falsify, conceal, or destroy evidence during an investigation or inquiry by the Commissioner.

Prosecution of PIPA offences

Regulatory offences tend to be “strict liability” offences, meaning that the Crown must only prove that the defendant committed the offence, not that the defendant acted with intent. A presumption is raised that the defendant acted negligently, which the defendant may rebut by proving that it acted reasonably.

Certain provisions in PIPA would seem to indicate that the Legislature intended the offences in PIPA to be offences of strict liability, but at the same time, some offences in the Act appear to require proof of intent.

The Committee heard that the offences in PIPA act as a deterrent, but to be effective, these offences must not be extremely difficult to prosecute. The Committee was advised that it is often difficult for the Crown to prosecute offences requiring proof of intent. The Information

and Privacy Commissioner's submission to the Committee proposed an amendment to the Act that would make the offences in PIPA strict liability offences.

Taking into consideration that PIPA requires organizations to act reasonably with respect to the protection of personal information, that the defence of reasonable care provides the opportunity to establish that the conduct in question was reasonable in the circumstances, and that there are certain established processes that ensure offences under the Act are prosecuted only in the most serious of cases, the Committee recommended:

44

That the Act be amended to change the standard required to find an offence under the Act from intentional to negligent.

Time limits for prosecutions

Instead of the present six-month time limit for the prosecution of offences under PIPA, the Information and Privacy Commissioner proposed an amendment that would extend the time limit to two years.

The Committee considered the circumstances and time frames in which contraventions of the Act are discovered and the processes for prosecuting an offence under Alberta privacy legislation as well as other provincial statutes. The Committee understood that other Alberta privacy statutes, as well as a number of other provincial statutes, have a two-year limitation period. The Committee also understood that the Commissioner considered two years to be a reasonable time to discover the offence, review the material, refer the matter to the Minister of Justice and Attorney General, and lay a charge. The Committee recommended:

45

That the Act be amended to provide a two-year limitation period for prosecution of offences.

Penalties under PIPA

PIPA permits the courts to impose a fine on a person found guilty of an offence under the Act. The fine must not exceed \$10,000 in the case of an individual and \$100,000 in the case of an organization. The Act does not include any special provisions with respect to fines or court orders.

The Committee considered a recommendation from the Information and Privacy Commissioner to allow the courts to direct a person convicted of an offence under PIPA to take some action that promotes the purposes of the Act, and to direct that a fine imposed under the Act be used for a program or activity that supports or promotes the purposes of the Act.

The Committee looked at the advantages that are thought to derive from directing fines to projects that serve the public interest. Organizations that have been guilty of negligence have an opportunity to make amends in a positive way, and judges are able to impose meaningful penalties that are well regarded by victims of offences, as well as the general public. The

Committee also considered the disadvantage of giving the courts the discretion to direct funds away from the General Revenue Fund. This might be seen to reduce transparency and accountability in the allocation and spending of such funds by taking them out of the annual appropriation process.

On balance, the Committee believed that the positive benefits of “creative sentencing” outweighed any disadvantages. On the understanding that funds would be provided to an organization operating a privacy program at arm’s length from government and from the Office of the Information and Privacy Commissioner, the Committee recommended:

46

That the Act be amended to allow the courts the discretion to direct that a fine imposed under the Act be used for a program or activity that supports or promotes the purposes of the Act.

Administration of the Act

The Committee considered whether any changes should be made with respect to the administration of the Act.

Review of the Act

The Government submission proposed an amendment which would extend the time between reviews to six years from the date that the Select Special Committee submitted its final report.

The existing review provision in PIPA requires a special committee of the Legislative Assembly to begin a comprehensive review of the Act by July 1, 2006, with reviews occurring at least once every three years after that. A report must be submitted to the Legislative Assembly within eighteen months after beginning a review.

The Committee considered the consensus among stakeholders that the Act is functioning well and provides effective privacy protection. Committee members also considered the time needed to implement amendments and assess their effectiveness. A concern was raised about addressing new information technologies that might emerge as threats to privacy between reviews, but there was a general confidence in PIPA, as an Act of general principles, to deal with new technologies.

The Committee was of the opinion that there is general support for the Act and that six years would allow for the amendment of the Act following a review and for assessment of the effect of amendments before a subsequent review. Believing that the Regulations should be addressed in a concurrent review process, the Committee recommended:

47

That the provision for review of the Act be amended to extend the time between reviews to six years from the submission of the report of the special committee and to add a requirement that a review of the Regulations will occur with each review of the Act.

Relation between the Act and the Regulation

The Government submission proposed a technical amendment to make PIPA more user-friendly with respect to the application of definitions under the Act.

After PIPA was passed, there was a need to more clearly define several words and phrases in the Act. These definitions were included in the PIPA Regulation. It had been suggested that it would be more convenient to have these definitions within the Act proper.

The Committee agreed that, where a definition applies to the Act or to a section of the Act, it would be more convenient to users if the definition appeared in the Act. The Committee recommended:

48

That definitions in the Regulation that apply to the whole Act, or to a section of the Act, be established in the definitions section of the Act or the relevant section, as appropriate, to bring them more easily to the attention of users.

Appendix A: Submissions to the Review Committee

Individual / Organization	
1.	Ms Colleen McMorran
2.	K&M Building Contractors Ltd.
3.	The Association of Professional Engineers, Geologists, and Geophysicists of Alberta
4.	Mr. Robert Hahn
5.	Ms Anne Burke
6.	Anglican Diocese of Edmonton and the Ecclesiastical Province of Rupert's Land
7.	CF 'Managing Movement'
8.	Alberta Real Estate Association
9.	The Alberta Association of Collection Agencies
10.	Petro-Canada
11.	Alberta Blue Cross
12.	College and Association of Registered Nurses of Alberta
13.	Child and Youth Care Association of Alberta
14.	Association of Canadian Financial Corporations
15.	Motor Dealers' Association of Alberta
16.	Alberta Construction Association
17.	Rocky Mountain College
18.	Alberta Association of Private Investigators
19.	IBM Canada Ltd.
20.	Alberta College of Medical Diagnostic and Therapeutic Technologists
21.	Canadian Condominium Institute, North Alberta Chapter
22.	ATB Financial
23.	Construction Labour Relations – An Alberta Association
24.	The Alberta Teachers' Association
25.	Association of School Business Officials of Alberta
26.	Equifax Canada Inc.
27.	First Canadian Title
28.	Alberta Opticians Association
29.	TransUnion of Canada, Inc.
30.	Independent Insurance Brokers Association of Alberta
31.	Alberta Land Surveyors' Association

32. College of Alberta Dental Assistants
33. Office of the Information and Privacy Commissioner of Alberta
34. Better Business Bureau of Southern Alberta
35. Merit Contractors Association
36. Canadian Federation of Independent Business
37. Alberta Medical Association
38. National Association for Information Destruction – Canada
39. Progressive Contractors Association of Canada
40. Roman Catholic Bishop of the Diocese of Calgary
41. Insurance Bureau of Canada
42. Consumers' Association of Canada (Alberta)
43. Ms Antoinette Belanger
44. Association of Records Managers and Administrators – Calgary Chapter
45. The Faculty Association of the University of Calgary
46. Alberta Dental Association and College
47. Mr. Allan Buteau
48. College of Physical Therapists of Alberta and College of Alberta Psychologists
49. Canadian Life and Health Insurance Association Inc.
50. EPCOR Utilities Inc.
51. Alberta Physiotherapy Association
52. The Law Society of Alberta
53. Canadian Bankers Association
54. Canadian Finance & Leasing Association
55. Real Estate Council of Alberta
56. Canadian Blood Services
57. Retail Council of Canada
58. Canadian Bar Association – Alberta
59. Syncrude Canada Ltd.
60. Cenera
61. Health Law Institute
62. Personal Information Protection Act Advisory Committee
63. Service Alberta, on behalf of the Government of Alberta
64. Ms Anne Landry
65. Ms Ida Mitten

Appendix B: Oral presentations to the Review Committee

Name	Organization
Mr. David Jones, Q.C.	Anglican Diocese of Edmonton and the Ecclesiastical Province of Rupert's Land
Ms Cindy Roberts	Canadian Bar Association – Alberta
Ms Wendy Armstrong Mr. Larry Phillips	Consumers' Association of Canada (Alberta)
Ms Val Mayes	Edmonton Chamber of Voluntary Organizations
Mr. Russ Dahms	Edmonton Federation of Community Leagues
Mr. Sheldon Greenspan Mr. Bob Johnson	National Association for Information Destruction – Canada
Mr. Frank Work, Q.C. Information and Privacy Commissioner	Office of the Information and Privacy Commissioner of Alberta
Mr. Paul Pellis, Deputy Minister	Service Alberta, on behalf of the Government of Alberta
Mr. Allan Buteau	
Ms Anne Landry	

Appendix C: Recommendations

Recommendations for amendments to PIPA

1. 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.
3. That the Act be amended to require organizations to notify the Office of the Information and Privacy Commissioner of a privacy breach involving personal information if the privacy breach meets certain criteria, and to notify affected individuals if directed to do so by the Commissioner, subject to the condition that there is an expedited process where notifying the individual is time-critical.
4. That the Act be amended to make it an offence not to notify the Office of the Information and Privacy Commissioner of a security breach affecting personal information, where it is reasonable to do so.
5. That the Act be amended to make PIPA apply fully to all not-for-profit organizations, subject to a one-year transition period.
9. That the Act be amended to provide that when an individual consents to the disclosure of personal information by an intermediary for a specified purpose, the individual is deemed to have consented to the collection by the receiving organization for the specified purpose.
10. That the Act be amended to allow an organization to deem an individual to consent to the collection, use and disclosure of his or her personal information for the purpose of coverage or enrolment under an insurance, benefit, or similar plan if the individual has an interest in or derives a benefit from that plan.
11. That the notification provision in the Act be amended to permit an organization to provide an individual with the position title or name of a person who can answer an individual's questions.
12. That the Act be amended to allow an organization to use and disclose personal information without consent for the purpose of an audit or inspection of that organization, and to allow an organization performing an audit or inspection to collect, use and disclose personal information for that purpose.
13. That the exception to consent for fraud prevention be amended to delete the current provision for market manipulation and unfair trading practices, and also that the exception be amended to expressly permit the disclosure of personal information by or to designated organizations – namely, the Insurance Bureau of Canada's Investigative Services and the Bank Crime Prevention and Investigation Office of the Canadian Bankers Association – for the purpose of fraud prevention.

-
15. That the exclusion for business contact information be amended to clearly enable an individual to be contacted in his or her capacity as an employee, including an official, of either a private-sector or a public-sector body.
 16. That the Act's provisions respecting publicly available personal information be amended to include a reference in each case to the meaning of this term that is prescribed in the Regulation.
 17. That the Act be amended to add the definition of "officer of the Legislature" that appears in the *Freedom of Information and Protection of Privacy Act*.
 18. That the Act be amended to expand the application of the provisions for "personal employee information" to the personal information of former employees.
 19. That the Act be amended to require organizations to collect, use and disclose employee references only with the consent of the individual the reference is about.
 20. That the definition of "employee" be amended to clarify that all provisions of the Act that apply to "employees" of an organization also apply to officials of an organization, and that the provision for business contact information be simplified to refer to "an employee of an organization."
 21. That the language of the provisions for collection, use and disclosure of personal information without consent be amended to clarify that an organization may collect, use or disclose personal information, including personal employee information, only for purposes that are reasonable and only to the extent that is reasonable for those purposes.
 23. That the Act be amended to include a provision allowing for deemed refusal of a request for access if an organization refuses to respond to the request, so as to allow the individual a right to request a review.
 26. That the reference to excusing payment of a fee be deleted from the Act's provisions respecting time limits for requesting a review, since the Act does not require an organization to consider a request to excuse payment of a fee.
 27. That the phrase "subject to the regulations" be deleted from the Act's provisions respecting fees for the correction of personal information, since regulations on this matter are not contemplated.
 29. That the Act be amended to require an organization to destroy or anonymize, within a reasonable time, personal information that an organization no longer requires for legal or business purposes, and to add a definition of destruction to the Act.

-
30. That the Act be amended to require an organization to retain records relating to an investigation by the Commissioner for at least one year after the conclusion of an investigation.
 31. That the provision requiring an organization to ensure the accuracy and completeness of personal information be amended to state that an organization must ensure that personal information is accurate and complete to the extent that is reasonable for the organization's purpose in collecting, using or disclosing the information.
 32. That the Act be amended to provide the Commissioner with explicit authority to discontinue an investigation or a review when the Commissioner believes the complaint or request for review is without merit or where there is not sufficient evidence to proceed.
 33. That the Act be amended to state that when information to which solicitor–client privilege applies is disclosed to the Commissioner at his request, this solicitor–client privilege is not affected.
 34. That a provision be added to the Act to allow the Commissioner to disclose to the Minister of Justice and Attorney General information relating to the commission of an offence under an enactment of Alberta or Canada if the Commissioner considers there is evidence of an offence, subject to the condition that the Commissioner must not disclose information that is subject to solicitor–client privilege.
 35. That the Act be amended to provide that all processes relating to a complaint or request for review must be completed within one year of receiving the complaint or request for review where practicable, with the Commissioner retaining the ability to extend timelines where necessary.
 36. That the Act be amended to explicitly state that neither the Commissioner nor anyone acting on his behalf or under his direction can be compelled to give evidence in a court or in any other proceedings, except as specified in the Act.
 37. That the Act be amended to delete the provision with respect to staying a Commissioner's order such that an organization must comply with an order of the Commissioner.
 38. That the Act be amended to provide that an application to a court for judicial review of a Commissioner's order must be made within 5 business days from the day that the person making the application is given a copy of the order.
 39. That the provision for orders that may be issued after inquiry be amended to allow the Commissioner not to issue an order, so as to remove the necessity of an order on a matter where none of the options for orders is applicable under the circumstances.

-
40. That the provisions referring to the Commissioner's powers to hold inquiries and make orders relating to access requests be amended, for consistency, to refer to requests for recorded personal information.
 41. That the provision for severing a request for review or complaint before providing it to other persons be amended to refer to the organization concerned and any other person *that will receive a copy of the request*.
 42. That the Act be amended to make it an offence to contravene the "whistleblower" protection provisions under the Act.
 43. That the Act be amended to make it an offence for a person to dispose of, alter, falsify, conceal, or destroy evidence during an investigation or inquiry by the Commissioner.
 44. That the Act be amended to change the standard required to find an offence under the Act from intentional to negligent.
 45. That the Act be amended to provide a two-year limitation period for prosecution of offences.
 46. That the Act be amended to allow the courts the discretion to direct that a fine imposed under the Act be used for a program or activity that supports or promotes the purposes of the Act.
 47. That the provision for review of the Act be amended to extend the time between reviews to six years from the submission of the report of the special committee and to add a requirement that a review of the Regulations will occur with each review of the Act.
 48. That definitions in the Regulation that apply to the whole Act, or to a section of the Act, be established in the definitions section of the Act or the relevant section, as appropriate, to bring them more easily to the attention of users.

Recommendations for other action

2. 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.
7. That a recommendation be made to the Minister of Health and Wellness that all personal information about individuals that is collected, used or disclosed for diagnostic, treatment or care purposes be brought within the scope of the *Health Information Act*, regardless of how these health services are funded.
8. That a recommendation be made to the Minister of Health and Wellness that, in cases where an amendment to the scope of the *Health Information Act* affects

organizations currently subject to PIPA, consideration be given to whether it is necessary to authorize personal health information to flow between custodians and organizations.

No change recommended

6. That the Act not be amended to add an exception to consent expressly allowing a religious organization to disclose a list of congregation members to a member to use for matters relating to the affairs of the congregation.
14. That the current language of the Act be maintained, which might require an organization to provide notice to an individual when collecting personal information directly from the individual where consent is not required.
22. That the definition of “personal information” remain unchanged, with no reference to “work product information,” so as to continue to allow an organization to consider the context when deciding whether information in a record created as part of an individual’s employment responsibilities is “personal information.”
24. That the exception for confidential information of a commercial nature not be amended at this time, allowing the matter of access to personal information in a succession, redundancy or restructuring plan to be addressed through the independent review process.
25. That the Act not be amended to add an express exception to access for personal information in a record that is subject to a solicitor’s lien.
28. That the provisions for personal information codes be maintained and the issue of modifying or deleting these provisions be revisited during the next review of PIPA.

There were a few instances where the Committee canvassed an issue but did not make a formal recommendation:

- Consistent approach to privacy legislation (p. 5)
- Regulation-making powers (p. 20)
- Continuing requests (p. 25)
- Fee schedule (p. 29)
- Commissioner’s power to compel documents subject to solicitor–client privilege (p. 35)
- Commissioner’s power to initiate audits of an organization (p. 38)
- Commissioner’s power to enter premises during an investigation or inquiry (p. 38)
- Offence to fail to make reasonable security arrangements (p. 42)

