SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT

Submission of the Office of the Information and Privacy Commissioner for British Columbia

March 2008

TABLE OF CONTENTS

PREFACE

This submission does not recommend a major change in direction for the *Personal Information Protection Act*. This reflects the fact that—as the clear majority of other submissions to the Committee illustrate—the *Personal Information Protection Act* is a balanced and effective law that requires no radical fix or overhaul. As might be said, "There's no need to fix what isn't broken." That said, this submission does suggest that the Committee recommend changes to PIPA that would improve its interpretation and application for organizations, individuals and our office.

In 2004, the federal Cabinet declared British Columbia's law to be substantially similar to the federal *Personal Information Protection and Electronic Documents Act*. Whatever the Committee decides to recommend, I respectfully suggest that it bear in mind the outcomes of the recent parliamentary reviews of that federal law and of Alberta's *Personal Information Protection Act*. In significant measure, the federal review resulted in recommendations that would bring the federal Act closer to the British Columbia and Alberta laws, but it is important that, in moving forward, the Committee have an eye on developments in, and flowing from, both the federal and Alberta reviews.

Portions of this submission respond to arguments by industry associations and other stakeholders. Our views are offered solely in the hope that they will be of some assistance. The Committee should know that I have written to stakeholders and offered to meet with them to discuss their concerns. The goal is to, where possible and as appropriate, assist with compliance challenges that their members face.

Of course, I would be happy to answer any questions the Committee might have about this submission or to assist in any way I can.

March 2008

David Loukidelis
Information and Privacy Commissioner
for British Columbia

1.0 Introduction

[1] This is the submission of the Office of the Information and Privacy Commissioner ("OIPC") to the Special Committee to Review the Personal Information Protection Act ("Committee").[1] This submission offers a general discussion of the importance of privacy, an overview of the *Personal Information Protection Act* ("PIPA"), highlights of the OIPC's experience to date in overseeing compliance with PIPA and the OIPC's recommendations for changes to PIPA.

[2] In considering amendments to PIPA, and in making its recommendations, the OIPC has acted with the following objectives in mind:

- Ensuring PIPA is achieving its stated purposes;
- Strengthening, where appropriate, the privacy rights of citizens;
- Reducing regulatory burden by simplifying legislative language;
- Harmonizing PIPA wherever possible with similar privacy legislation in other Canadian jurisdictions, notably Alberta and federally-regulated sectors and jurisdictions; and
- Simplifying, expediting and strengthening the compliance oversight powers and processes.

[3] Because PIPA is, overall, a well balanced and successful law, no overhaul is recommended or desired. It has achieved its stated purpose of governing the collection, use and disclosure of personal information by private sector organizations in a manner that recognizes both the right of individuals to protect their personal information and the need for organizations to use that information for reasonable purposes.

[4] Recent reviews by legislators of both the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and the Alberta *Personal Information Act* ("Alberta PIPA") recommended changes that would further harmonize those laws with British Columbia's in critical areas. The outcome of those reviews, and developments flowing from them, are an important context for the Special Committee's deliberations.

2.0 The Importance of Privacy

[5] The term "privacy", which is not defined in British Columbia legislation, has different definitions. To some it means the "right to be let alone". This is the classic definition of privacy provided in 1890 by Louis Brandeis, later a justice of

[1] Under s. 59 of PIPA, an all-party special committee of the Legislative Assembly was established by resolution on April 19, 2007 to review PIPA and submit a report including any recommended amendments to PIPA or any other Act.

the United States Supreme Court. To others, it means anonymity, while still others believe it means the right to be unobserved. Privacy is certainly a rich concept with several dimensions. It includes the right to control access to your physical space, your body, your thoughts, your communications and your information.

[6] A pernicious yet enduring myth is that privacy matters only to those who have something illegal or wrong to hide. Most of us have nothing to hide, yet still attach great value to our individual privacy. Privacy matters because we all have the right to maintain a private life, separate and apart from our public life. We negotiate our identity in the world and choose to share pieces of ourselves with those we trust.

[7] More than this, the essence of liberty in a democratic society is the right of individuals to autonomy, to be generally free from state and corporate interference in their lives. The freedom of citizens to choose, subject to demonstrably necessary and carefully tailored limits, what information they share with others is one of the fundamental differences between totalitarian states and free society.

[8] Privacy matters, in other words, because it restrains the appetite of governments and law enforcement agencies, but also private sector actors:

> People who have no rights of privacy are vulnerable to limitless intrusions by governments, corporations, or anyone else who chooses to interfere in your personal affairs. Imagine a world where government had an unfettered right to demand information from you, or to remove money from your bank account, or even to enter your house. The tragic history of many of the world's countries shows us that a nation denied the right of privacy is invariably denied all other freedoms and rights.[2]

[9] Privacy matters because our physical and emotional well-being requires it. Imagine going to your doctor, dentist, family counsellor, priest or employee assistance counsellor without any confidence that the information you supplied during those sessions would remain private.

[10] Privacy also matters because our economy depends on it. Imagine going to a bank for a loan, to a lawyer to draw up a will, to a financial planner, to a property management company to rent an apartment, or to the internet to purchase a book online without any guarantees that the information you provided would be respected and kept confidential. As recent years have shown, the costs of fraud, identity theft and other misuse of our personal information are real, substantial and mounting. These losses harm individuals, but they can also harm economic activity and growth.

---

[2] Simon Davies, *Big Brother* (Pan MacMillian Publishing, UK, 1997).

[11] Surveys consistently and emphatically affirm that Canadians believe privacy matters. A survey of Canadian attitudes towards privacy commissioned by the Privacy Commissioner of Canada and released in the fall of 2007 paints a worrisome picture.

[12] A large proportion of Canadians continue to worry about their privacy and have high expectations of strong privacy laws. They think that businesses and the government need to take their privacy responsibilities more seriously. Canadians overwhelmingly expect to be notified in the event of a breach. The majority feel that they should be notified regardless of the sensitivity of the information. Seven out of ten of Canadians perceive having less protection of their personal information than they did ten years ago. Two of every three Canadians hold the view that protecting the privacy of Canadians will be one of the most important issues facing the country over the next ten years.[3]

[13] This real fear translates into consumer behaviour that erodes healthy social values and detracts from the corporate bottom line. Gartner Research estimates that consumer reluctance to shop online due to privacy and security concerns has taken $2 billion out of the economy[4] and the Canadian Medical Association estimates that fully 11% of patients withhold vital health information from their own physicians because of privacy concerns.[5] The fall-out of concern about privacy is an erosion of consumer trust. In the face of privacy fears, consumers shop elsewhere or, certainly in the online context, provide fake, inaccurate and incomplete information.

[14] Privacy matters and is year in, year out a vital public policy concern. Governments around the world have therefore passed privacy laws over the last 40 years in the public and, more recently, private sectors. In Canada, legislators have moved within the past 15 years to protect privacy in the private sector.[6] Here in British Columbia, a private sector law came about in no small part because of the vision of British Columbia's legislators. In 2001, an all-party special committee of the Legislative Assembly unanimously recommended enactment of a law regulating the private sector's collection, use and disclosure of personal information.[7] The committee recognized that British Columbia businesses and consumers solidly supported legislation in the private sector:

---

[3] "Canadians and the Privacy Landscape", EKOS research Associates Inc., sponsored by the Office of the Privacy Commissioner of Canada, March 2007.

[4] Gartner: Web security fears cause $2 billion online commerce loss since 2006", SC Magazine, November 28, 2006.

[5] "Canadian Perceptions of Health Information Confidentiality", Canadian Medical Association/ Angus Reid Survey, 1999.

[6] Quebec's private sector privacy law came into force in 1994. The federal Personal Information Protection and Electronic Documents Act was passed in 1999 and came into force in stages beginning in 2001.

[7] Report of the Special Committee on Information Privacy in the Private Sector, Legislative Assembly of British Columbia (2001). www.leg.bc.ca/cmt/36thParl/priv_ps/Reports/IPPS-36-4-Report.pdf.

> The Committee heard that British Columbians are in fact concerned about information privacy and support its regulation. Businesses want privacy rules to help them build trust with consumers and clients, and they want to operate in a regulatory environment that is consistent for all businesses in all jurisdictions. Consumers want their personal information to be used properly and only by those who need to use it. The concerns of some individuals and organizations incorporate the wide implications of private sector information use for both individuals and society as a whole, especially its impact on the human and civil rights that enrich our society. The Committee learned that concerns like these are common to individuals, businesses, advocates and legislators throughout the information society. Western nations have responded by developing a set of fair information principles that can be applied to private sector activities in order to maintain both information privacy rights and businesses' ability to use personal information for legitimate purposes.[8]

[15] In recommending the adoption of a made-in-British Columbia private sector privacy law, the committee adopted some guiding principles. First, the committee wrote, any law must be substantially similar to the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA'). Second, the legislation must be based on the ten internationally recognized "fair information practices", which uphold an individual's right to reasonable control of the collection, use and disclosure of his or her personal information. Third, our privacy law must be harmonized among jurisdictions in which private sector organizations do business.

3.0 Basic Rules of Private Sector Privacy

[16] PIPA is essentially a privacy roadmap. It contains a set of internationally recognized rules—called fair information practices or principles—that govern the collection, use and disclosure of personal information.[9] Under PIPA, privacy means maximizing, wherever possible and to the extent reasonable, a citizen's control over the collection, use and disclosure of his or her personal information. PIPA itself reflects the balance between informational self-determination and other public interests:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[10]

---

[8] Report of the Special Committee on Information Privacy in the Private Sector, p. 7.

[9] These principles are most famously articulated in the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, to which Canada is a signatory. They are also found in the Canadian Standards Association Model Code for the Protection of Personal Information (Q830), which forms Schedule 1, and the core, of PIPEDA.

[10] PIPA, s. 2.

[17] PIPA applies to "personal information", which it defines as information about an "identifiable individual".[11] It does not apply to the collection, use or disclosure of personal information for personal, home or family purposes (for example, for Christmas card mailing lists of family and friends), for artistic or literary purposes or for journalistic purposes (this protects freedom of expression for the news media).

[18] Consistent with the international fair information principles, PIPA sets out ten rules governing how organizations may collect, use, disclose and secure personal information. These rules require an organization to:

1. Identify the purpose for which personal information is collected, at or before the time the information is collected.
2. Obtain consent for the collection, use and disclosure of personal information.
3. Collect only as much personal information as is necessary to fulfill the stated purposes.
4. Limit the use, disclosure and retention of personal information to the purposes for which it was collected.
5. Ensure personal information is accurate for the purposes for which it was collected.
6. Upon request, provide an individual with access to his or her personal information.
7. Make reasonable security arrangements to protect personal information from such risks as unauthorized, collection, use, disclosure and retention.
8. Designate someone who is responsible for ensuring an organization complies with the law.
9. Develop policies and procedures necessary to meet legal privacy obligations.
10. Develop a process for resolving complaints about the failure of an organization to live up to its privacy obligations.

[19] Before addressing the substantive issues, the following section outlines the OIPC's role under PIPA and offers an overview of the relevant experience in overseeing compliance with PIPA.

[11] PIPA does not apply to "business contact information" or "work product information", terms defined in the law and discussed further below.

4.0 A Snapshot of Four Years of Enforcement

[20] Headed by the Information and Privacy Commissioner ("Commissioner"), an officer of the Legislature, the OIPC was established in 1993 to provide independent review of access to information decisions and privacy-related activities of public bodies covered by the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The Commissioner is also responsible for overseeing compliance with PIPA by more than 300,000 provincially-regulated for-profit and not-for-profit private sector organizations, including businesses, charities, religious organizations, associations, trade unions and trusts. Under PIPA, the OIPC is empowered to:

- Investigate and resolve complaints that personal information has been collected, used or disclosed by an organization in contravention of PIPA;
- Initiate investigations and audits to ensure compliance with PIPA if the Commissioner believes there are reasonable grounds that an organization is not complying, including issuing binding orders;
- Inform the public about PIPA;
- Conduct or commission research into anything affecting the achievement of the purposes of PIPA;
- Comment on the privacy implications of programs, automated systems or data linkages proposed by organizations;
- Authorize the collection of personal information from sources other than the individual to whom the personal information relates; and
- Investigate and resolve complaints that a duty imposed by PIPA has not been performed, an extension of time has been improperly taken, a fee is unreasonable or a correction request has been refused without justification.

[21] When PIPA came into force, the OIPC dedicated significant resources to building compliance capacity across the broad spectrum of organizations covered by PIPA. In collaboration with business associations and colleagues in Alberta, in particular, the OIPC developed guidebooks, guidelines, information sheets, template documents and other implementation tools for organizations. These included core documents such as guidance on how to investigate a privacy complaint and how to develop a privacy policy. To take other examples, the OIPC developed guidelines for the public on how to ask organizations for their own personal information, how to file complaints and how to raise a privacy issue directly with the organizations involved. The *Guide to PIPA for Businesses and Organizations* was designed for small to medium size businesses, as was the resource document entitled *PIPA and the Hiring Process:*

Frequently Asked Questions. Businesses responded favourably to these support tools, which we continue to supplement and update.[12]

[22] The OIPC also has worked cooperatively and collaboratively with the Office of the Information and Privacy Commissioner of Alberta and the Office of the Privacy Commissioner of Canada to, wherever possible, harmonize investigative and interpretive approaches and to align our processes to reduce regulatory overlap and burden. To this end, senior officials from each of these three offices, and from Quebec's Commission d'accès à l'information, participate in regular conference call meetings of the four offices' Private Sector Privacy Forum. Further, a memorandum of understanding to affirm and elaborate upon the co-operative relationship is being prepared for the commissioners' consideration. This document would replace the existing January 2004 letter of understanding among the three commissioners.

[23] As for the substance of the OIPC's work under PIPA, the bulk of it involves investigating complaints from individuals about the collection, use, disclosure, retention, safeguarding and access to their personal information. For the last four calendar years, the OIPC has, on average, received about 200 of these each year.

[24] The OIPC will generally defer or adjourn acting on a complaint until the individual concerned shows that he or she has communicated directly with the organization and enabled it to respond to or attempt to resolve the matter. When the OIPC does take a complaint, the approach is similar to that taken for FIPPA complaints. OIPC staff will investigate the circumstances of the dispute, consider the application of relevant sections of PIPA to those circumstances and involve the individual and the organization in efforts to arrive at a mediated resolution. Individuals or organizations that are dissatisfied with the results of mediation have the option of asking the Commissioner to conduct an inquiry. The OIPC's complaint process has resulted in high resolution rates for privacy complaints, with relatively few formal orders being necessary in the past four years.

[25] The most common category of personnel-related complaints is complaints by employees of small businesses about their employers' information practices or, more commonly, former employees seeking their own personal information. Employees of larger organizations frequently call the OIPC for information about PIPA, but are often able to resolve their issues directly with their employers.

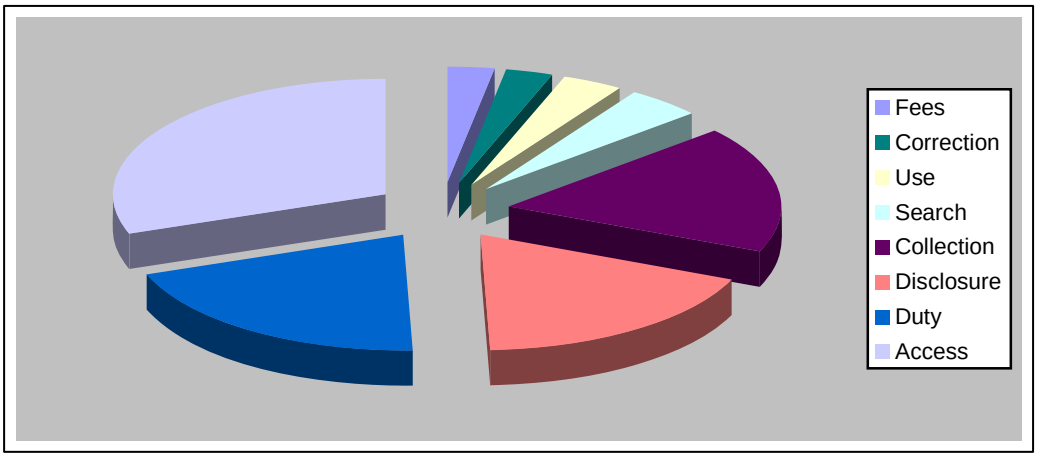
[26] The types of industries that receive the most complaints include finance and insurance, strata corporations, real estate rental services, consumer goods rentals, administrative services such as collection agencies and credit bureaus, health care and social assistance services.

---

[12] All OIPC guidance documents and information are found on the OIPC website, www.oipc.bc.ca.

[27] The nature of the disputes filed over the last four calendar years is broken down as follows:

Nature of PIPA Disputes
(January 1, 2004 – December 31, 2007)



[28] Again, the vast majority of these disputes have been resolved without resorting to a formal inquiry or requiring an order by the Commissioner. In four years, only eleven matters have been resolved through a formal inquiry and seven more matters are currently at hearing. The orders issued to date have given guidance on when organizations can require customers to provide personal information as a condition of doing business with them, set standards on retention periods for personal information, interpreted PIPA's concept of "work product information", limited the disclosure of employee personal information only to those that have an operational need-to-know, confirmed the ability of an organization to withhold information protected by solicitor-client privilege (including litigation privilege) and prohibited the use, without prior notice and consent, of personal information for secondary marketing purposes.

5.0 OIPC Recommendations

5.1 Mandatory Notification of Privacy Breaches

[29] Data is becoming a new currency of crime. According to the RCMP Commercial Crime Branch, from January 1, 2004 to December 31, 2006 there were 32,125 victims of identity theft in Canada and the value of the loss reported was $44 million dollars.[13] The federal Department of Justice identifies identity theft as one of the fastest growing problems in Canada and states that, in 2006, almost 8,000 victims of reported losses of $16 million. Furthermore, the

[13] "Canada's New Government To Tackle Identity Theft", Department of Justice Canada Media Backgrounder, October 2, 2007.

Canadian Council of Better Business Bureaus has estimated that identity theft and other forms of bank and credit card fraud cost Canadian businesses more than $2 billion annually.[14]

[30] While hacking has risen dramatically in the last ten years, the OIPC's experience and external research both support the conclusion that the unauthorized use or disclosure of personal information—known as a privacy breach—is often the result of insider error or malfeasance. A survey published last year of 127 companies in the US found that 54% of those that had experienced a privacy breach said it was caused by employee failure to adhere to privacy rules.[15]

[31] A study done by the University of Washington concluded that human error was the main culprit in the loss of sensitive personal information in 61% of breaches, and that the primary source of data loss was the loss of laptops and mobile devices.[16] One survey concluded that the primary reason data breaches occur is that companies do not even know what sensitive data they have on their systems or where it resides within their networks.[17]

[32] Notable sources of privacy breaches that have come to the attention of the OIPC include:

- Unauthorized browsing of personal information by employees;
- Insecure storage or care of personal information (*e.g.*, laptops left in plain sight in cars or coffee shops, files left in hotel rooms);
- Insecure disposal of personal information (including mobile devices, storage media and hard drives);
- Employees' failure to comply with privacy rules;
- Inadequate or non-existent privacy training; and
- Failure to monitor access to personal information.

[33] Surveys consistently underscore the real concern of the public around the security of their personal information and the risks of misuse by organizations, their employees and by criminals. As indicated earlier, recent polling done for the Office of the Privacy Commissioner of Canada affirms these concerns and the impact they can have on customer and employee trust in businesses.

---

[14] *Ibid*.
[15] "Survey: Employees Are Biggest Threat to Data Security", Martin H. Bosworth, Consumer Affairs.com, June 28, 2006.
[16] "Forget Hackers: Companies responsible for most data breaches, study stays", Jaikumar Vijayar, Computerworld Security, March 14, 2006.
[17] "US Survey" Confidential Data At Risk", Ponemon Institute, LLC, sponsored by Vontu Inc., San Francisco, August 15, 2006.

[34] Organizations also have a legal obligation to protect customer and employee information. Section 34 of PIPA requires an organization to protect "personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure copying, modification or disposal or similar risks." What protective measures are "reasonable" depends on many factors, including the likelihood of the risk, the seriousness of the harm that might result, the cost of prevention and established custom.

[35] The Commissioner may order an organization to implement appropriate safeguards. An individual may also recover from an organization actual losses in the Supreme Court of British Columbia if the Commissioner has issued an order finding that the organization has breached PIPA. This latter remedy is costly and difficult to pursue.

[36] To date, the OIPC has focussed on supporting organizations in responding to privacy breaches and in avoiding them. OIPC publications on privacy breaches[18] identify and provide guidance on four key steps for responding to privacy breaches:

- Contain the breach by, for example, stopping the unauthorized practices, shutting down a compromised database or recovering records;

- Evaluate the risks caused by the breach, taking into the account the nature of the personal information compromised, the uses to which the information could be put, the causes and extent of the breach and the foreseeable harm;

- Notify affected individuals in appropriate circumstances, as soon as possible; and

- Once the immediate steps to mitigate the risks associated with the breach have been completed, thoroughly investigate the cause of the breach and develop or improve safeguards.

[37] Regarding the third step, the factors that must be taken into consideration in deciding whether or not to notify include whether:

- Legislation requires notification;
- Contractual obligations require notification;
- Notification would harm a law enforcement investigation;
- There is a risk of identity theft or fraud;

[18] OIPC resources can be found at this link: www.oipc.bc.ca/sector_private/resources/index.htm.

- There is a risk of physical or mental harm;
- There is a risk of humiliation or damage to someone's reputation; and
- There is a risk of loss of business or employment opportunities.

[38] Where notice to affected individuals is warranted, timeliness is critical in order to enable them to take action to minimize the risk of financial damage or other harm.

[39] PIPA does not expressly require an organization to notify affected individuals if the security of their personal information has been compromised. The Commissioner has, in the past, publicly questioned whether an explicit duty to notify affected individuals is necessary. This position has been influenced, in part, by the Commissioner's view that s. 34 of PIPA imposes such a duty in appropriate circumstances.

[40] Some organizations have made submissions to the Committee that no statutory duty to notify should be created, while others have called for enactment of a duty. As indicated in other submissions to the Committee, a variety of factors might suggest that PIPA should be clarified by including an express duty to notify in carefully specified circumstances:

- A specific duty to notify would remove any uncertainty about the existence of the duty for organizations that are not familiar with the full import of s. 34;
- The explicit duty could provide specificity about the range of circumstances in which notification is or is not required, thus avoiding unnecessary expense for organizations and notification fatigue for individuals;
- The number and scale of ongoing privacy breaches might suggest that organizations need a more direct incentive to comply with their statutory duty to protect personal information. Publicity flowing from notification of breaches could shine the light of public scrutiny on organizations with poor practices, thus giving them a market-based incentive to keep customer loyalty by staying out of the news; and
- Recently completed legislative reviews of PIPEDA and of Alberta's PIPA have yielded unanimous recommendations for reform in this area.[19] As noted earlier, ongoing substantial similarity between PIPA and PIPEDA is necessary. Further, harmonization between PIPA and these other two laws is desirable in order to avoid inconsistency for organizations and individuals alike. For this reason alone, an amendment of PIPA in this area merits serious consideration.

[19] In addition, more than 40 states in the US have enacted mandatory breach notification laws, with California's security breach notification law being one of the better-known laws. See *California Civil Code*, 1798.29 and 1798.82, accessible through: http://www.leginfo.ca.gov/calaw.html.

[41] The OIPC does not support a duty to notify affected individuals of all privacy breaches, regardless of the nature of the personal information involved or the degree of risk. Too broad a duty to notify would almost certainly lead to over-notification, which would entail considerable expense for organizations, could result in notification fatigue for individuals and could in some situations unnecessarily alarm individuals.

[42] Any amendment should specify which kinds of personal information must be involved before the duty to notify arises, risk factors that must be considered when assessing the requirement to notify and the timing and methods of notification. Any amendment should require that these breaches be reported to the OIPC and that the Commissioner be given the authority to order an organization to notify affected individuals where the organization has failed to do so. The submission of the Freedom of Information and Privacy Association and BC Civil Liberties Association, addressed below, has a useful discussion of the various factors and considerations in this area.

[43] The OIPC would oppose any amendment requiring it to decide in all cases when notification is required, to determine the particulars of notification or to carry out notification. The OIPC believes this is not an appropriate role for it to play and is deeply concerned about the resource implications it carries.

[44] As noted above, the OIPC has in the past questioned the need for an express duty to notify in PIPA. The OIPC takes the view that s. 34 of PIPA already requires, in appropriate cases, organizations to notify affected individuals and believes s. 34 offers flexibility in this regard. That said, the OIPC recognizes that an express notification duty could provide clarity and certainty to organizations and individuals. Further, both the PIPEDA and Alberta PIPA reviews have recommended enactment of express notification duties and the federal government has indicated that it will move ahead with legislation. On balance, therefore, the OIPC recommends that, in the interests of harmonization alone, PIPA remain aligned with developments in those jurisdictions by including an express requirement to notify in carefully defined and controlled circumstances.

Recommendation 1––PIPA should be amended to include an express duty for organizations to notify affected individuals of unauthorized disclosure or use of their personal information, but the amendment should be carefully crafted so as to be effective, not over-broad. To that end, the amendment should address the following considerations:

(a) the kinds of personal information that must be involved before notice may be required, with personal information that is likely to create risks of financial loss or fraud being a key consideration;

(b) who must be notified (affected individuals and the OIPC, with a possible added requirement to notify credit reporting agencies or law enforcement agencies in cases where financial loss is a risk);

(c) how notice is to be given;

(d) the timing of the giving of notice;

(e) the general content of notices; and

(f) authority for the Commissioner to order an organization to notify affected individuals of a privacy breach, on conditions the Commissioner may specify, where the organization has not given notice and the Commissioner considers that PIPA requires it.

5.2 Solicitor Client Privilege Is Well Protected

Determining claims of solicitor-client privilege

[45] The Law Society of British Columbia ("LSBC") has raised the question of whether the Commissioner's powers to examine documents in order to verify whether they are subject to solicitor-client privilege may be at odds with protection of the privilege.

[46] PIPA gives the Commissioner responsibility for complaints and reviews about the application of the statutory exemptions to an individual's right of access to personal information. The exemptions include s. 23(3)(a), which allows an organization to refuse to disclose personal information in response to an individual's request for access to her or his own personal information if it is protected by "solicitor-client privilege". To enable the Commissioner to perform the function of verifying the proper application of exemptions, the Legislature conferred express powers and duties to conduct inquiries in private, to require the production of documents for examination and to review the information at issue in strict confidence. Section 38 therefore empowers the Commissioner to compel the production and examination of documents where an individual's access to personal information has been denied. Section 38(3) expressly specifies that disclosure of a document to the Commissioner does not affect any solicitor-client privilege that applies to it.

[47] The LSBC's concern that the Commissioner's jurisdiction to examine privileged documents may be inconsistent with s. 3(3) of PIPA is not well founded. Section 3(3) provides that nothing in PIPA affects solicitor-client privilege. Section 3(3) stands apart from s. 3(2), the list of subject matters to which PIPA does not apply. Section 3(2) does not exclude organizations engaged in the practice of law or documents protected by solicitor-client privilege from the scope of the legislation; nor does s. 3(3). On the contrary, s. 3(3) is a harmonious confirmation of the provision in s. 38(3) that solicitor-client privilege is not affected by disclosure to the Commissioner for the purpose of determining

whether s. 23(3)(a) has been properly applied by an organization. There is, therefore, no inconsistency between s. 3(3) and s. 38 of PIPA.

[48] The Commissioner has had the power to examine and where necessary compel production of records protected by solicitor-client privilege for fifteen years in the public sector and four years in the private sector. It is well known and accepted that confidential examination is a necessary tool for determining claims of solicitor-client privilege.[20] Such records are examined solely to verify the asserted privilege and, as the Commissioner said in Order 00-08,[21] examination for that sole purpose is never undertaken gratuitously.

[49] The LSBC has also suggested that the decision of the Supreme Court of Canada in *Goodis v. Ontario (Ministry of Correctional Services)*[22] may undermine the propriety of the Commissioner's examination of documents for the purpose of determining the validity of an organization's claim that they are protected by solicitor-client privilege. *Goodis* is not apposite, however, because it involved the question of disclosure of privileged records to counsel for an interested party—the requester seeking access to information—to assist in arguing the question of whether the privilege was properly claimed.

[50] This is obviously a very different exercise than the process the Legislature has mandated under PIPA for disclosure to the Commissioner for the sole purpose of neutral and independent verification of the asserted privilege. The Commissioner is not an interested party and examines the documents only to determine the validity of the claimed privilege. The Commissioner does not use the documents to make them public or for any other purpose. If the Commissioner makes an order deciding against the privilege claim, the Commissioner does not disclose the documents. The order is directed to the organization, it is subject to an application for judicial review in the Supreme Court of British Columbia and it is stayed from the time the judicial review application is filed until the court orders otherwise.[23]

[51] There is no cause for concern around s. 3(3) of PIPA or the *Goodis* decision. The mechanism in British Columbia for allowing the Commissioner to examine records claimed to be subject to solicitor-client privilege for the sole purpose of verifying that claim has worked very well and no amendment is necessary to fully protect the privilege.

---

[20] *Foster Wheeler Power Co. v. Société intermunicipale de gestion et d'élimination des déschets (SIGED) Inc.*, [2004] 1 S.C.R. 32, para. 47, and *G.W.L. Properties Ltd. v. W.K. Grace & Co. of Canada*, [1992] B.C.J. No. 1761 (S.C.), p. 5.

[21] Order 00-08, [2000] B.C.I.P.C.D. No. 8, paras. 29-35 (reversed on a different ground, *College of Physicians of British Columbia v. (British Columbia) Information and Privacy Commissioner)*, [2002] B.C.J. No. 2779 (CA).

[22] [2006] 2 S.C.R. 32.

[23] PIPA, s. 53.

Litigation privilege is already protected

[52] The Insurance Bureau of Canada ("IBC") has recommended that s. 23(3)(a) of PIPA, which authorizes an organization to refuse to disclose personal information to an individual that "is protected by solicitor-client privilege", be amended to specifically refer to "litigation privilege". This change is not necessary because the reference to "solicitor-client privilege" in s. 23(3)(a) already incorporates both legal professional privilege and litigation privilege. This has been the long-standing interpretation of the same language in s. 14 of FIPA, by the Commissioner and by the courts, and that interpretation has already been applied in several orders the Commissioner has issued under PIPA. In Order P06-02,[24] for example, the Commissioner confirmed his decision in Order P06-01[25] that the phrase "solicitor-client privilege" is to be interpreted to include both kinds of privilege, legal professional privilege and litigation privilege. This interpretation of s. 23(3)(a) is consistent with numerous British Columbia court decisions[26] affirming that "solicitor-client privilege" encompasses both kinds of privilege as well as Supreme Court of Canada jurisprudence to the same effect. An amendment to s. 23(3)(a) is not necessary to incorporate litigation privilege.

Recommendation 2––The provisions of PIPA dealing with solicitor-client privilege, including the provisions empowering the Commissioner to examine records claimed to be privileged, should not be amended. Nor is any amendment necessary to protect the privilege.

5.3 Employee Personal Information

[53] Under PIPA, "employee personal information" is personal information that is reasonably required to establish, manage or terminate a work relationship. It does not include personal information about employees held by an organization that is not related to those things. Employee personal information is a distinct category of personal information and PIPA has special rules for collection, use and disclosure of "employee personal information".[27]

[54] PIPA's rules about "employee personal information" do not apply to former employees. To give only one example, the way PIPA now reads, where an employer needs to disclose personal information of former employees to pay them post-employment benefits such as pensions, the employer would have to

[24] [2006] B.C.I.P.C.D. No. 28; URL: http://www.oipc.bc.ca/PIPAOrders/2006/OrderP06-02.pdf.
[25] [2006] B.C.I.P.C.D. No. 5; URL: http://www.oipc.bc.ca/PIPAOrders/2006/OrderP06-01.pdf.
[26] See, for example, *College of Physicians and Surgeons v. British Columbia (Information and Privacy Commissioner)*, [2002] B.C.J. No. 2779 (C.A.). Also see *Blank v. Canada (Minister of Justice)*, [2006] SCC 39, [2006] SCJ No. 39. The IBC refers to *Blank*, but does not note that the decision involved an interpretation of s. 23 of the federal *Access to Information Act*, specifically that the term "solicitor-client privilege" incorporates both types of privilege.
[27] Employee personal information does not include business contact information or work product information.

obtain the consent of the former employees.[28] The OIPC doubts this was intended by the Legislature and recommends an amendment to permit non-consensual use and disclosure of "employee personal information" after termination of the employment relationship. The amendment would have to be carefully tailored, however, to limit it to situations where the use or disclosure is necessary to manage post-employment relations or dealings between the employer and former employee. The OIPC notes that the Alberta legislative review committee made such a recommendation (Recommendation 18).[29]

Recommendation 3––PIPA should be amended to permit non-consensual use and disclosure of "employee personal information" after termination of the employment relationship. The amendment should be carefully tailored to limit it to situations where the use or disclosure is necessary to manage post-employment relations or dealings between the employer and former employee.

5.4 Streamlining the Dispute Resolution Process

[55] In 2004, the OIPC made a number of recommendations to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* ("FIPPA Review Committee") that were intended to streamline and simplify the processes for complaining or appealing to the OIPC under FIPPA. Recommendation 20 of the FIPPA Review Committee's unanimous May 2004 report[30] reads as follows:

> 20. Amend the Act to combine the complaint process and the review and inquiry process—referred to in sections 42(2) and 52(1) respectively—into a unitary process for the Commissioner to investigate, mediate, inquire into and make orders about complaints respecting decisions under the Act or other allegations of non-compliance with the Act.

[56] Recommendation 20 has yet to proceed, although there has been no suggestion to the OIPC's knowledge that the government opposes that recommendation.[31]

[57] Similar amendments to PIPA are necessary because, as the Commissioner indicated in his appearance before the Committee last May, Parts 10 and 11 of PIPA place unnecessary burdens, and real costs, on the

---

[28] Section 8(2)(a) of PIPA, which dispenses with consent respecting benefit plans, would not necessarily cover the case of the employee, as opposed to a third-party beneficiary.

[29] www.assembly.ab.ca/committees/reports/PIPA/finalpipawReport111407.pdf.

[30] *Enhancing the Province's Public Sector Access & Privacy Law* (2004), www.leg.bc.ca/CMT/37thParl/session-5/foi/reports/Rpt-FOIPPA37-5.pdf

[31] Some of the Special Committee's process-oriented recommendations were contained in Bill 25-2007, the *Labour and Citizens' Service Statutes Amendment Act*, which received First Reading in 2007. Recommendation 20 was not included in Bill 25, which has not, in any case, proceeded any further at the time of writing.

OIPC and on individuals and organizations involved in processes under PIPA. The following discussion by the Commissioner in Order P07-01, which regrettably merits extensive quotation to drive home the point, illustrates the unnecessarily convoluted, and often obscure, nature of these aspects of PIPA:[32]

> [39] Some candid observations are in order about the provisions in Part 11 and other parts of PIPA that govern the OIPC's processes. These are to put it mildly not a model of simplicity or clarity. The definitions, intertwining terminology and tortured linking of provisions in Parts 10 and 11, which are reproduced in the appendix to this order, are particularly challenging to interpret.
>
> [40] Section 45 defines "complaint" in Part 11 to mean a complaint referred to in s. 36(2), which is the commissioner's authority to, without limitation of the powers under s. 36(1), investigate and attempt to resolve a wide variety of complaints. Section 36(1)(a) gives the commissioner authority to initiate investigations and audits to ensure compliance with any provision of PIPA, whether a complaint is received or not, but only if satisfied there are reasonable grounds to believe that an organization is not complying with the legislation. Section 36(2), in contrast, does not incorporate a requirement for reasonable grounds to believe that an organization is non-compliant. Section 36(2) also does not specify who may make a complaint.
>
> [41] Sections 45, 46 and 47 distinguish between conducting a review and making or resolving a complaint. The conduct of a review is tied to a request by an individual for access to or correction of her or his own personal information. Under s. 47(2), any request for a review that does not involve an organization's failure to respond within a required time period must be made within 30 days of notice of the circumstances upon which the review is based, or a longer period allowed by the commissioner. Making or resolving a complaint is tied to an individual and to the meaning of complaint in s. 36(2). Under s. 47(3)(b), a request to resolve a complaint need not be made within any prescribed time.
>
> [42] The complaint jurisdiction under s. 36(2), particularly ss. 36(2)(a) and (d), is wide enough to encompass review of a decision resulting from an individual's request for access to or correction of his other personal information. Therefore, on the face of it, a concern of that type could be brought as a complaint or as a review. Against any apparent logic, there would be no prescribed time limit to bring the matter as a complaint but there would be a prescribed 30-day time limit to bring the same matter as a review. It is true that, under s. 47(2)(b), the commissioner could relax the time period for a request for review to be delivered, but if the commissioner refused to do this, the matter could still be brought anyway as a complaint.
>
> [43] The wording of s. 36(1)(b) introduces more needless complexity and uncertainty because it empowers the commissioner to "make an order described under section 52(3), whether or not a review is requested" but

[32] [2007] B.C.I.P.C.D. No. 32.

> not, evidently, whether or not a complaint has been made. This means that, for a case about an organization's decision, act or failure to act respecting access to or the correction of an individual's personal information, the commissioner may make an order under s. 52(3) even if a review is not requested, but not under s. 52(2) even though the relief in s. 52(2) could well be relevant in such a case. Further, if the commissioner were to investigate that same matter, or any other matter, without having received a complaint about it, then he or she could make no order under s. 52 at all. As if this were not enough, the s. 45 definition of the meaning of "review" in Part 11 clearly invites the question of whether "review" could have a different meaning in s. 36(1)(b), found in Part 10 of PIPA.
>
> [44] Worse still, s. 45 creates a definition of "request" in Part 11 that, in relation to complaints, means a request made in writing under s. 46 to resolve a complaint. Section 46(2) refers to making a complaint. Section 47(1) refers to making a complaint by delivering a request and s. 48(2) refers to receiving a request respecting a complaint. The lamentable upshot of these various definitions and inconsistent terminology is that unreal distinctions are created between making a complaint and requesting it to be resolved.
>
> [45] There are also different prescribed time frames for the completion of complaints as contrasted with reviews under Part 11. Under s. 50(6) and (7), if a complaint is referred to inquiry, the time frame for completion of the inquiry is 30 days after the end of mediation or, if there is no mediation, after the delivery of the request. Under s. 50(8), if a review is referred to inquiry, the timeframe for completion of the inquiry is 90 days from delivery of the request or longer as specified by the commissioner.

[58] The public and organizations expect and should enjoy an accessible, unambiguous and streamlined complaint, investigation and adjudication process under PIPA. Consistent with the FIPPA Review Committee's 2004 recommendation for a unitary approach under FIPPA, the OIPC urgently recommends a unitary approach under PIPA, entailing the scrapping of Parts 10 and 11 and a complete re-build. The OIPC also believes that there should, as far as possible, be one set of processes under FIPPA and PIPA for resolving any complaint, whether in the public or private sector.

[59] The OIPC asks the Committee to make a recommendation respecting PIPA that is the same in substance as recommendation 20 of the 2004 FIPPA Review Committee and urges the Committee to call on the government to move forward quickly with consistent FIPPA and PIPA amendments. In 2005, the Commissioner offered the provincial government a ready-made draft of a new Part 5 of FIPPA, which would implement the FIPPA Review Committee's recommendation. This could also form the basis for the revamped PIPA

provisions requested here. To assist the Committee, the 2005 draft is set out in the Appendix to this submission.[33]

[60] As regards FIPPA, the OIPC notes that the FIPPA Review Committee unanimously recommended these changes almost four years ago, yet there has been no progress with these vital, uncontroversial changes.

Recommendation 4––PIPA should be amended to make the complaint and review processes into a unitary process of the same nature as that recommended in 2004 by the Special Committee to Review the Freedom of Information and Protection of Privacy Act. The PIPA amendments should proceed hand in hand, as quickly as possible, with the comparable FIPPA amendments recommended in 2004.

6.0 Comments on Other Submissions

6.1 FIPA & BC Civil Liberties

[61] The BC Freedom of Information and Privacy Association ("FIPA") and the BC Civil Liberties Association ("BCCLA") have made a joint submission to the Committee (collectively, "FIPA/BCCLA"). Both organizations are important stakeholders in access to information and privacy law and policy matters. They have played important roles in promoting open public debate and in promoting compliance with the law. The OIPC acknowledges their contributions.

[62] The FIPA/BCCLA submission has expressed concern about "weak standards and a lack of clarity in PIPA concerning openness requirements" and has suggested that "timid enforcement" by the OIPC has in some cases prevented individuals from receiving "a written privacy policy and a thorough description of policies and practices."[34] They have suggested that PIPA's language should be clarified and strengthened with an amendment that matches the standards in Part 4.8 of Schedule 1 to PIPEDA.

[63] In Order P06-04, the commissioner held that s. 5(c) of PIPA does not require an organization to make a written privacy policy publicly available or available to an individual on request. In that case, the organization said that it would verbally discuss its privacy policy with non-employees upon request, but without actually providing a written copy of the policy. The organization acknowledged that it had a written privacy policy, but said that s. 5(c) did not

[33] Versions of some of the provisions set out in the appended draft Part 5 were included in Bill 25-2007, the *Labour and Citizens' Services Statutes Amendment Act, 2007*, which received First Reading during the last Session of the Legislative Assembly. These amendments would have implemented some, but not all, of the 2004 FIPPA Review Committee recommendations, with the balance being implemented later.

[34] FIPA/BCCLA submission, p. 6.

require it to provide a copy on request. In view of the legislative language used in s. 5(c), the commissioner said the following:

> [73] Section 5(c) says an organization must "make information available on request about" its "policies and practices" developed under s. 5(a) and about the "complaint process" required under s. 5(b). An organization may find that it is easier to simply hand over a copy of its privacy policy or complaint process than to answer questions or otherwise make information available. There is certainly a good business case for organizations to be transparent with customers, employees and others with whom they deal. Openness about good practices and policies will foster trust and thus loyalty, which can translate into repeat business and perhaps even lower employee turnover.
>
> [74] There is, however, no duty under s. 5(c) for an organization to provide anyone a copy of any written policies and procedures, on request or otherwise. The legislative language is clear. It only requires organizations to make "information about" policies, practices and processes available on request. This interpretation both respects the clear legislative language of s. 5(c) and accords with the legislative intent underlying PIPA.
>
> [75] The complainant asked questions of Fox about privacy concerns the complainant had and about alleged breaches of PIPA. The questions, which would almost certainly have entailed detailed answers, went beyond a request for information about policies, practices and processes under s. 5. PIPA does not require an organization to make other information available, but that is what the complainant expected of Fox. If the complainant wanted to complain to Fox about its practices, the complainant could have done so using the complaint processes required under s. 5(c), but, assuming for discussion purposes only that Fox failed to answer the complainant's questions, any such failure was not in these circumstances a breach of s. 5(c).

[64] In this light, FIPA/BCCLA has submitted that the openness principle underpinning modern privacy legislation is not upheld "unless an organization's privacy policy, practices and complaint process are clear, comprehensive and easily accessible." The OIPC agrees with FIPA/BCCLA, but notes that a statutory duty to make written privacy policies publicly available might have a significant impact on many small businesses and volunteer community organizations that are active in British Columbia. They are now required to have such policies and to make information about them available, but the OIPC is on balance not sure that a broad, or unqualified, duty to make them publicly available in writing is desirable.

Cross border data flows and accountability

[65] While recognizing that restrictions on the export of personal information are neither practical nor desirable, FIPA has submitted that the accountability standard at present enshrined in s. 4(2) of PIPA is inadequate. It notes that

clause 4.1.3 of Schedule 1 to PIPEDA goes further by requiring organizations that transfer personal information to third parties for processing—or for the provision of services, one could add—to use contractual or other means to provide a comparable level of protection while the information is being processed or held by the third party. The OIPC therefore supports the portion of FIPA/BCCLA recommendation 7 that addresses the accountability issue, *i.e.*, recommendations 7(a) and (b).

[66] The OIPC does not, however, support the other portions of FIPA/BCCLA recommendation 7. The Alberta PIPA review committee recommended an amendment to require organizations to notify individuals when their personal information is being transferred to a third-party service provider outside Canada (Recommendation 1). While an organization might decide to do this as a matter of good customer relations, a legal obligation to notify would not, in the OIPC's view, advance the accountability principle.

[67] It would also, in any event, be all but meaningless in our world of ubiquitous, ever-shifting cross-border data flows. An email containing personal information may well cross several international borders on its way to a business partner a block away. Individuals who post their own personal information on a website are transferring it across borders. Would notice of data export be required in such cases? Since cross-border data flows are now routine, complex and constantly shifting, the OIPC believes a notice requirement would lead to generic language about possible cross-border flows being inserted into organizations' overall notice and consent process for customers. The Committee may wish to consider the degree to which this would assist consumers.

Recommendation 5––To provide clarity, s. 4 of PIPA should be amended, consistent with PIPEDA, to state that:

(a) organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and

(b) organizations must use contractual or other means to ensure compliance with PIPA, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization.

6.2 Canadian Bar Association (BC Branch)

[68] The British Columbia Branch of the Canadian Bar Association ("CBA") represents approximately 6,000 lawyers who practice law in many different areas. The CBA's Freedom of Information and Privacy Law Section is an active forum for the exchange of information and ideas, and for debate, about access to

information and privacy law issues. The OIPC acknowledges the CBA's important role in promoting understanding of and compliance with PIPA.

[69] As the CBA has noted in its submission to the Committee, it has solicited and communicated to the Committee input from CBA members as opposed to presenting a unanimous or majority submission.

No exception for "without prejudice" discussions

[70] Some CBA members believe there should be an exception to an individual's right of access to her or his own personal information respecting communications that have been sent "without prejudice" in the context of settlement discussions in litigation or labour relations grievances. It is argued that such an exception would promote full and frank discussion of issues and resolve early resolution of disputes. The OIPC does not see how this limitation on an individual's right of access is necessary to encourage early settlement of disputes. The OIPC is aware of no evidence that the right of access has been exercised in a way that prolongs disputes or prevents their resolution.

Business transactions

[71] Section 20 of PIPA permits certain non-consensual disclosure and use of personal information about "employees, customers, directors, officers or shareholders" of an organization in the context of a business transaction. Some CBA members consider that the categories of personal information that may be disclosed or used extend beyond the classes of information that PIPA at present specifies. As examples of other kinds of personal information, the CBA mentioned personal information of candidates for employment and of employees of other organizations. The OIPC acknowledges the concern that the existing categories of personal information, being limited to "employees, customers, directors, officers and shareholders", may be unduly restrictive such that s. 20 does not fully implement the legislative intention underlying the provision. The OIPC recommends that PIPA be amended to address this concern.

Recommendation 6––Section 20 of PIPA should be amended to provide that an organization may disclose or collect personal information in its custody or under its control (including personal information about its employees, customers, directors, officers or shareholders) without consent as otherwise provided by s. 20.

Cross-border data flows

[72] The CBA has said in its submission that any amendments to PIPA imposing restrictions or requirements on cross-border data flows may result in inconsistency amongst Canadian privacy laws and the creation of unnecessary barriers to commerce and economic development. As the Commissioner has publicly stated on a number of occasions, the public policy issues connected with

cross-border data flows in relation to the outsourcing of public services differ from considerations prevailing in relation to private sector cross-border data flows.[35] This difference was at the heart of the OIPC's 2004 report *Privacy & the USA Patriot Act—Implications for British Columbia Public Sector Outsourcing*.[36]

[73] The OIPC would not support an amendment to PIPA that imposed restrictions or controls on the export of personal information from British Columbia to elsewhere in Canada or abroad. Such an amendment would leave PIPA out of step with other Canadian private sector privacy laws. It would emulate a European model of personal information export restrictions that is widely acknowledged as being outmoded and unworkable.[37] The accountability obligation under s. 4(2) of PIPA is sufficient, particularly if elaborated upon as recommended above, to ensure that personal information an organization exports from British Columbia is protected by sufficient arrangements (whether contractual or otherwise).

6.3 Canadian Bankers Association

[74] The Canadian Bankers Association represents banks whose banking subsidiaries may be provincially regulated. It has suggested that PIPA be amended to authorize the OIPC to decline to investigate complaints that do not merit the resources required to do so.[38] The Canadian Bankers Association has suggested such an amendment to federal government policy makers in relation to PIPEDA. The Privacy Commissioner of Canada, Jennifer Stoddart, has requested such an amendment to PIPEDA and the legislative review of Alberta PIPA resulted in a similar recommendation (Recommendation 32).

[75] The Commissioner's discretion under PIPA to investigate complaints and requests for review enables the Commissioner to create policies respecting when the OIPC will decline to open an investigation or decline to proceed further with a complaint where a file has been opened. These policies could include situations where a case lacks merit or is of such a nature that the resources necessary to investigate are not warranted.

[76] In view of the Alberta and federal developments on this front, and to provide clarity to individuals and organizations, the OIPC recommends that PIPA

---

[35] The commissioner articulated this perspective in Order P06-04. Also see the Commissioner's speech, *Transborder Data Flows & Privacy—An Update On Work In Progress*. www.oipc.bc.ca/pdfs/Speeches/TransborderDataFlowsSpeech(10Feb06).pdf.

[36] www.oipc.bc.ca/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final.pdf.

[37] The export restriction approach taken in the 1995 European Union Directive on personal information protection reflects a time when cross-border data flows tended to be point to point or batch processing transfers. The rise of the internet and e-commerce has changed the landscape dramatically. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, O.J,L 281, 23 Nov.,1995, P. 0031 – 0050.

[38] Some members of the Canadian Bar Association's Freedom of Information and Privacy Law Section also suggested such an amendment.

be amended to expressly provide the Commissioner with discretion in this regard. This amendment would be part of the overhaul of Parts 10 and 11 of PIPA recommended above. Section 55.1 of the draft of a new Part 5 of FIPPA, appended to this submission, sets out the OIPC's recommended approach.

Recommendation 7––PIPA should be amended, in order to provide greater clarity for individuals and organizations, to give the Commissioner discretion to decline to open a complaint investigation or to dismiss a complaint if the Commissioner is satisfied that one or more of the following applies:

(a) the request for review is not within the jurisdiction of the Commissioner;

(b) the request for review was not delivered within an applicable time limit;

(c) the request for review is frivolous, vexatious or trivial or gives rise to an abuse of process;

(d) the request for review was made in bad faith or for an improper purpose or motive;

(e) the person that asked for the review failed to diligently pursue the review or failed to comply with an order or direction of the commissioner in relation to it;

(f) there is no reasonable prospect the request for review will succeed;

(g) the subject matter of the request for review could be or has been appropriately dealt with in another proceeding or process;

(h) a fair and reasonable remedy or resolution to all or part of the request for review has been

(i) provided or made available by the public body to the person that asked for the review, and

(ii) the person that asked for the review has failed to accept the remedy or resolution;

(i) no meaningful remedy is available under the Act.

6.4 Insurance Bureau of Canada

[77] The Insurance Bureau of Canada ("IBC") is the national trade association representing private sector general insurers. The IBC has been very active, across Canada, in privacy-related matters. It has worked with privacy commissioners' offices across the country in promoting good privacy practices

and compliance with privacy legislation by insurance industry participants. The OIPC acknowledges and appreciates the IBC's assistance and support with PIPA compliance in the insurance industry.

Witness statements and an insured's consent

[78] The IBC has argued that the need for an insured's consent to collection of witness statements may harm an insurer's handling of claims and any resulting litigation. There is no reason why consent could not be built into the contract of insurance. The insured would consent, through the terms of the insurance policy, to the insurer collecting personal information in the form of statements by witnesses to an accident or other events giving rise to an insurance claim by the insured.

[79] If the insured later tried to revoke that consent, as s. 9(1) of PIPA permits, the insurer could invoke policy terms denying coverage. Section 9(3) of PIPA prevents an organization from prohibiting withdrawal of consent, but nothing in s. 9 says that the organization must nonetheless perform its side of the bargain if the withdrawal of consent frustrates the bargain. This is underscored by s. 9(2), which requires an organization to inform individuals of the likely consequences of withdrawing consent—here denial of coverage.

[80] Further, in cases where the insurer has grounds to believe that the insured is making a false claim or otherwise has breached the insurance policy, or any law, ss. 12, 15 and 18 of PIPA authorize the insurer to collect, use and disclose personal information without consent where it is reasonable to expect that obtaining consent "would compromise an investigation or proceeding" and the collection, use or disclosure "is reasonable for purposes related to an investigation or a proceeding." Section 1 of PIPA defines "investigation" as follows:

> **"investigation"** means an investigation related to
>
> (a) a breach of an agreement,
>
> (b) a contravention of an enactment of Canada or a province,
>
> (c) a circumstance or conduct that may result in a remedy or relief being available under an enactment, under the common law or in equity,
>
> (d) the prevention of fraud, or
>
> (e) trading in a security as defined in section 1 of the Securities Act if the investigation is conducted by or on behalf of an organization recognized by the British Columbia Securities Commission to be appropriate for carrying out investigations of trading in securities,
>
> if it is reasonable to believe that the breach, contravention, circumstance, conduct, fraud or improper trading practice in question may occur or may have occurred… .

Access to one's own personal information is vitally important

[81] The IBC's apparent suggestion that the right of access to one's own personal information is solely for the purpose of requesting its correction does not fully capture the importance of the access right.[39] The right of access enables individuals to learn what personal information an organization has about them so they can determine whether it is inaccurate or incomplete and request correction, but it also empowers individuals to look after their own interests in other ways. The access right can allow individuals to decide whether an organization has inappropriately collected too much information about them, used properly collected information in an inappropriate way, disclosed personal information inappropriately or retained personal information for too long. The importance of the right of access to one's own personal information is difficult to overstate.

Whose information is in a witness statement?

[82] The IBC has suggested that PIPA's definition of personal information be amended to clarify that personal information "expressed" by a witness about another individual is the personal information of the witness.[40] The IBC has also recommended that ss. 12, 15 and 18 of PIPA be amended to provide that an organization may, during the course of investigating and settling contractual issues or claims for loss of damages, collect, use and disclose a witness statement without the subject's knowledge or consent.

[83] The OIPC does not support these recommendations. The first recommendation, regarding witness statements and personal information, runs counter to the well-established position under other Canadian private sector privacy laws and is contrary to the public policy underpinnings of PIPA itself. It would also be inconsistent with the public policy underpinning FIPPA. One of PIPA's main purposes, and features, is that it gives individuals a right of access to their own personal information in the custody or under the control of an organization. This is an internationally-recognized principle and is a key part of any modern privacy law.

[84] Witness statements often contain factual observations by the witness about another individual's actions or behaviour, as well as qualitative comments about the nature and propriety of those actions. To statutorily decree that, by definition, witness statements are the personal information of the witness alone is artificial and inconsistent with the reality of such statements.

[85] Consistent with this observation, a recent Federal Court of Appeal decision under PIPEDA held that records of a medical examination of an insured conducted by a doctor retained by the insurer contained personal information of

[39] IBC submission, p. 3.
[40] IBC Submission, p. 3.

the insured, as well as possibly the doctor, who had expressed opinions about the insured's health.[41] This illustrates that a particular record or file may contain personal information of more than one individual and that a single piece of information may be the personal information of more than one individual.[42]

[86] Section 23(4)(c) of PIPA provides that, where an individual seeks access to his or her own personal information, the organization must not disclose the personal information of someone else. From a policy perspective, if PIPA's definition of personal information were amended to provide that witness statements are the personal information of the witness, the result would be that s. 23(4)(c) would prevent an individual who is the subject of a witness statement from gaining access to that information, which common sense says is information about that individual. This would be so even if the statement included, for example, deliberately false allegations about the individual. To statutorily bar individuals who are the subject of such statements from learning what others have said about them is contrary to PIPA's legislative goals. Nor has the IBC offered evidence that the existing PIPA definition of personal information has presented real obstacles for insurers in protecting their commercial interests. The OIPC is aware of no such evidence.

No new barriers to individuals' access

[87] The IBC has suggested that a new s. 23(3)(g) be added to PIPA to authorize organizations to refuse to disclose personal information "generated in the course of the process to investigate and settle contractual issues or claims for loss of damages." The wording of the IBC's proposed s. 23(3)(g) is on its face very broad. It appears to be an attempt to extend back in time a concept similar to litigation privilege and to expand it to effectively prevent individuals from ever gaining access to their own personal information in the hands of insurers, whenever a process has been engaged to "settle contractual issues" or to settle damage or loss claims. The OIPC opposes this recommendation. Nor has the IBC made the case that there is a need for such a sweeping change, which has not been recommended in relation to Alberta PIPA or in relation to PIPEDA.

[88] The IBC[43] has also recommended that PIPA be amended such that, when litigation has begun, "the provincial rules of civil procedure should govern and prevail over the access provisions in PIPA."[44] The rules of civil procedure that offer qualified access to one's own personal information in the hands of opposing

[41] *Rousseau v. Canada (Privacy Commissioner)*, [2008] F.C.J. No. 151, 2008 FCA 39.
[42] Another good example of an individual person being entitled to see what was said about him by others, including the names of the individuals who said those things, is *Canada (Information Commissioner) v. Canada (Ministry of Citizenship and Immigration),* [2002] FCA 270 F.C.J. (C.A.).
[43] The same recommendation has been made by the Canadian Life and Health Insurers Association. The OIPC opposes that recommendation for the reasons given here.
[44] IBC submission, p. 4.

litigants, for the purposes of the litigation, apply to proceedings in the Supreme Court of British Columbia, not the Provincial Court.

[89] It has been suggested on occasion over the years that FIPPA should be amended so that the civil discovery process supplants any rights of access to information, including to one's own personal information. These suggestions have not moved forward and the two legislative review committees for FIPPA recommended no such changes.

[90] The OIPC believes no case of real need has been made for this significant change and opposes this recommendation, which has not been made in either the federal or Alberta privacy law review processes.

Disregarding access requests

[91] Section 23 of PIPA permits an individual to request access to his or her own personal information in the control of an organization and s. 24 authorizes an individual to ask an organization to correct errors or omissions in the individual's personal information. Section 37 of PIPA reads as follows:

> **Power to authorize organization to disregard requests**
>
> 37 If asked by an organization, the commissioner may authorize the organization to disregard requests under section 23 or 24 that
>
> (a) would unreasonably interfere with the operations of the organization because of the repetitious or systematic nature of the requests, or
>
> (b) are frivolous or vexatious.

[92] The IBC says that "experience" shows

> …that some individuals are misusing the access and correction provisions of PIPA not as a means of insuring their privacy rights and protecting their personal information, but instead as a means to frustrate legitimate business purposes and to prevent the full facts of an incident from being collected and used.[45]

[93] The IBC's specific recommendation is that s. 37 should be amended to add two new heads of authority for the Commissioner to authorize organizations to disregard requests under s. 23 or s. 24. It notes that s. 37 of Alberta PIPA allows the Alberta commissioner to authorize organizations to disregard requests that "would amount to an abuse of the right to make those requests" and that s. 46 of Quebec's privacy legislation permits the Quebec commissioner to authorize organizations to disregard requests that "are not consistent with the purpose of the Act".

[45] IBC submission, p. 5.

[94] During the four-year period from January 1, 2004 to December 31, 2007 the OIPC received just three s. 37 applications from organizations, two of which were successfully mediated and one of which led to Decision P05-01.[46] In Decision P05-01, the Commissioner relied on an earlier FIPPA decision to interpret the phrase "frivolous or vexatious" in s. 37(b) as involving one or more of the following factors:[47]

- A frivolous or vexatious request is one that is an abuse of the rights conferred under PIPA;
- Determination of whether a request is frivolous or vexatious must, in each case, keep in mind the legislative purposes of PIPA;
- A "frivolous" request is one that is made primarily for a purpose other than gaining access to information;
- The class of "frivolous" requests includes requests that are trivial or not serious; and
- The class of "vexatious" requests includes requests made in "bad faith", *i.e.*, for a malicious or oblique motive. Such requests may be made for the purpose of harassing or obstructing the organization.

[95] This means the concept of abuse of the right to make access requests is encompassed by the s. 37 concept of "frivolous or vexatious" requests and any request that is frivolous or vexatious is not "consistent with the purpose" of PIPA.

[96] Acknowledging that such an amendment would further align PIPA with Alberta PIPA, the OIPC does not oppose an amendment as suggested by the IBC, noting that Recommendation 7, above, incorporates such concepts and is consistent with the thrust of the IBC's recommendation.

Access means access

[97] The IBC says it is

> …unclear from PIPA, and from the longstanding practice in this area that has developed with the public sector privacy laws, whether an organization must provide access to the actual documents in which the personal information is recorded or whether it can prepare a summary of the personal information, thus eliminating the inefficiency of the current approach of photocopying all of the documents. Some organizations may prefer to create this new document.[48]

[98] The OIPC opposes this recommendation.

---

[46] [2005] B.C.I.P.C.D. No. 23; URL: http://www.oipc.bc.ca/PIPAOrders/2005/DecisionP05-01.pdf.
[47] [2002] B.C.I.P.C.D. No. 57; URL: http://www.oipc.bc.ca/orders/section43/Auth(s.43)02-02.pdf.
[48] IBC submission, pp. 5-6.

[99] First, PIPA is not "unclear" on this point. It is clear beyond doubt that the right of access under PIPA is a right of access to personal information and not to a summary of personal information. Under s. 23(1) of PIPA, an organization must provide an individual who requests it with "the individual's personal information under the control of the organization". There is no ambiguity here. Section 23(1) clearly requires an organization to provide access to the "individual's personal information", subject to any severing under s. 23, not access to a summary.[49]

[100] In any event, the suggestion that organizations should be given the option, in their sole discretion, of refusing access to personal information and providing some sort of summary—the IBC does not suggest any criteria to govern this proposed new authority, which would be open to abuse—runs counter to PIPA's purposes. As noted above, an individual's right of access to her or his own personal information is a key component of any respectable privacy law because that right empowers individuals to monitor for themselves an organization's compliance with PIPA. The crucial right of access could be rendered meaningless by a new right for an organization to summarize personal information, not provide access.

[101] The OIPC notes that nothing in PIPA prevents insurers from offering their customers summaries of insurance claims files—these are the kinds of files the IBC has said are problematic—on an optional basis. If an insurer were to offer claims file summaries as an option, they might prefer that. As long as the insurer did not ignore an access request made under PIPA, this alternative arrangement would be acceptable and could improve customer relations.

Fees for access

[102] The IBC has expressed concern that s. 32(2) of PIPA only authorizes organizations to charge individuals a "minimal fee" for access to their own personal information. It notes that s. 32(1) of Alberta PIPA authorizes organizations to charge a "reasonable fee". The OIPC is concerned that PIPA is inconsistent on the issue of fees. Section 32(2) permits an organization to charge a "minimal fee", yet s. 36(2)(c) gives the Commissioner power to investigate whether a fee is "reasonable". This divergence in drafting is not easily explained. Noting that Alberta PIPA permits the charging of a "reasonable" fee, the OIPC supports the IBC's suggestion that s. 32(2) be amended to provide clarity, by substituting "reasonable" for "minimal".

Recommendation 8––Section 32(2) of PIPA should be amended to permit organizations to charge a "reasonable fee" for access by an individual to her or his own personal information.

[49] Further, there would be no need for the s. 23 exemptions from disclosure if the Legislature meant to require organizations to provide only summaries.

Work product information

[103] The IBC has suggested that PIPA's definition of "work product information" be amended to refer to information that is "prepared or compiled", as opposed to information that is "prepared or collected", by an individual or a group of individuals during the discharge of their employment duties. Although it has no reason to believe this is a pressing concern, the OIPC does not object to this suggestion. However, if the Committee recommends any change, it should be to add "compiled" to the existing list, not to substitute it for "collected".

6.5 Canadian Life & Health Insurance Association

[104] The Canadian Life and Health Insurance Association ("CLHIA") represents insurers who account for almost all life and health insurance business in Canada. The CLHIA has been active in working with privacy commissioners on issues that its members face under Canadian privacy laws and the OIPC acknowledges the contributions of the CLHIA.

[105] Two of the issues addressed in the CLHIA's submission are discussed above—breach notification and discovery of documents during civil litigation. The CLHIA also has suggested amendments to PIPA respecting individuals' access to their own personal health information.

Access to one's own personal health information

[106] Although the CLHIA acknowledges that individuals should have access to their own personal health information, it contends that, where health information is of a sensitive nature, it can only be fully understood and properly explained by a medical practitioner. The CLHIA contends that there "will be many occasions where the individual may need support when receiving the information", such that the information should be provided only by a medical practitioner.[50] It notes that the insurance industry has customarily disclosed medical information through the individual's medical practitioner, not directly to the individual. It cites Clause 4.9.1 of Schedule 1 to PIPEDA, which gives a disclosing organization the discretion to "choose to make sensitive medical information available through a medical practitioner."[51] The CLHIA contends that this approach "would be more appropriate" and that it would be in the best interest of customers if insurers are given the discretion to choose how to make personal health information available.

[107] As the CLHIA acknowledges, s. 23(4)(b) of PIPA and s. 5 of the Personal Information Protection Act Regulations recognize the need to protect the health

[50] CLHIA submission, pp. 7 and 8.
[51] CLHIA submission, p. 8.

and safety interests of individuals who seek their own personal information. Section 5 of the regulation authorizes an organization to obtain an assessment by a health care professional of whether disclosure to an individual of his or her personal information could reasonably be expected to result in grave and immediate harm to the individual's safety or mental or physical health.

[108] A similar standard has applied under FIPPA since 1994. The OIPC is aware of no evidence that the present approach under PIPA either jeopardizes individual health or safety or affects the interests of health or life insurers in British Columbia. Accordingly, the OIPC sees no need for the proposed amendment, which is not necessary in order to further align PIPA and PIPEDA. In any event, the OIPC sees no reason why an insurer would be precluded from adopting the approach advocated by the CLHIA under the existing PIPA framework if the individual consents to disclosure through her or his medical practitioner.

6.6 United Auto Trades Association

[109] During the February 6, 2008 presentation to the Committee of the United Auto Trades Association ("UATA"), UATA representatives referred to a complaint to the OIPC about the Insurance Corporation of British Columbia ("ICBC"). They appeared to suggest on several occasions that the OIPC has failed to investigate the complaint, which was made in June 2005, in a timely way. During that appearance, the Committee's Chair told the UATA's representatives that the Chair would seek information from the OIPC about why the complaint had not been moved forward. The Commissioner provided the Chair with that information in a February 13, 2008 email.

[110] In view of the UATA's testimony to the Committee about its complaint, the OIPC notes the following, for the record, respecting the complaint:

- The UATA's complaint to the OIPC was made in June of 2005;
- The matter was assigned to a Portfolio Officer, who investigated the complaint and decided, in writing, that the complaint was not substantiated;
- The UATA was not satisfied with this outcome and requested a reconsideration by the OIPC;
- A reconsideration is being conducted by the OIPC's Executive Director over approximately the last 10 months; and
- ICBC and the UATA have filed several submissions and reply submissions, the last being filed on January 11, 2008. Once she has completed her deliberations, the Executive Director will issue her decision.

6.7 Canadian Medical Protective Association

[111] The Canadian Medical Protective Association ("CMPA") is a not-for-profit mutual defence organization operated by and for medical practitioners. It is the main provider of medical-legal assistance to Canadian doctors, with some 10,000 members in British Columbia.

[112] One thrust of the CMPA's submission is that PIPA does not "expressly recognize the important role the CMPA and other similar organizations perform for patients and health care professionals with respect to medical-legal advice, error reduction and risk management activities" (original emphasis).[52] As general-purpose private sector privacy legislation, PIPA does not expressly recognize the roles of any other insurers or advisers either.

CMPA services can be accessed now

[113] The CMPA believes it is important that doctors not "feel that privacy legislation prohibits them from contacting the CMPA for the purpose of obtaining legal or risk management advice."[53] The CMPA's first specific concern is that PIPA requires a physician to obtain patient consent to share personal information that the physician wishes to share to obtain advice or support from the CMPA, but where no claim has been made or is anticipated. The CMPA suggests a new s. 18(1)(q) to address its concerns.

[114] The OIPC believes physicians should be able to obtain CMPA services in an effective manner under PIPA's existing provisions. PIPA defines "personal information" as information about an "identifiable individual". In many, if not all, cases a physician will be able to disclose to the CMPA enough information about a case to obtain services, but without identifying the patient involved. This will be so whether the CMPA-physician communications are verbal or written (and acknowledging that anonymization of recorded patient information may require effort on the part of physicians' offices).

[115] Further, at least as regards the error reduction and risk management activities of the CMPA, a physician could notify patients, and obtain their consent, to disclosure of personal information necessary to obtain CMPA services in these two areas. Not all patients would consent, of course, but this option does exist.

[116] The OIPC notes that neither the Alberta nor federal legislative reviews include recommendations in this area. The CMPA has not offered evidence of any pressing problem with PIPA's current language. The OIPC does not support the CMPA's recommendation to the Committee.

---

[52] CMPA Submission, p. 2
[53] CMPA Submission, p. 1.

Reasonably contemplated proceedings

[117] The CMPA has also suggested that PIPA's definition of "proceeding" be amended to cover anticipated proceedings and that ss. 15(1)(c) and 18(1)(c) be amended to permit use and disclosure of personal information where it is "reasonable for purposes related to an investigation or a proceeding". The OIPC does not object to amendment of the term "proceeding" to include proceedings in "reasonable contemplation" (not "anticipated" proceedings, as the CMPA suggests).

[118] The OIPC does have concerns about the CMPA's proposed ss. 15(1)(c) and 18(1)(c) amendments. At present, these provisions authorize, respectively, non-consensual use and disclosure of personal information where "it is reasonable to expect" that use or disclosure "with the consent of the individual would compromise an investigation or proceeding" and the use or disclosure "is reasonable for purposes related to an investigation or a proceeding". The CMPA would eliminate the requirement that obtaining consent could reasonably be expected to compromise the investigation or proceeding.

[119] The consent of individuals to the collection, use and disclosure of their personal information is at the core of PIPA and any departure from that default principle should proceed only where it is shown to be clearly necessary to address a pressing objective or concern. The CMPA has not shown that the present test of compromise of an investigation or proceeding has impeded efficient and effective investigation and defence of claims by the CMPA or others. The OIPC acknowledges that the provisions of Alberta PIPA comparable to ss. 15(1)(c) and 18(1)(c) are very similar to the CMPA's proposal, but the OIPC does not believe that the harm test in our PIPA should be eliminated.[54]

6.8 Xtract Inc.

[120] According to its website, Xtract Inc. ("Xtract") "is an internet-based solution to the problem of checking items deposited at pawn and second-hand shops against stolen property reports."[55] Xtract appears to be in the business of selling database software to law enforcement agencies.

[121] As the OIPC understands the testimony of Xtract's representative before the Committee, Xtract believes that customer personal information must be provided to police by pawnshop and second-hand stores in order to combat property theft in British Columbia. Xtract appears to have suggested that customer personal information should routinely and automatically be communicated to police—for every transaction, for every customer—regardless of the circumstances.

---

[54] Alberta PIPA, ss. 17 and 20. These permit use or disclosure without consent where it "is reasonable for the purposes of an investigation or a legal proceeding".

[55] http://www.xtract.ca/.

[122] Xtract referred to communicating names to police along with property serial numbers, but referred also to the apparent great success in identifying stolen property through transmission of serial numbers alone. As Xtract's own website notes, "it is estimated that fifty percent (50%) of identified stolen merchandise, made through electronic reporting software, comes from serial number hits" alone.[56] In this light, it is not clear why personal information of all customers should be routinely and without cause disclosed to police unless and until stolen property is identified and case-specific follow-up is warranted.

[123] As regards recent developments in this area, the OIPC notes that, under Ontario's *Municipal Freedom of Information and Protection of Privacy Act*, the Information and Privacy Commissioner of Ontario ordered the City of Ottawa to cease routine collection of customer personal information from pawnshops. This occurred after the Ontario Court of Appeal struck down a City of Oshawa bylaw on the basis that it conflicted with the Ontario *Municipal Freedom of Information and Protection of Privacy Act*. Last month, Alberta's Information and Privacy Commissioner prohibited routine collection of customer personal information by the City of Edmonton and its disclosure to police. Here in British Columbia, in 2007 the Court of Appeal struck down a City of New Westminster bylaw requiring routine transmission to police of customer personal information, on the basis that the bylaw was not authorized by the *Community Charter*.[57]

[124] As the Committee's chair indicated at the conclusion of Xtract's appearance, the questions raised by Xtract relate to other laws. In 2006, the OIPC issued a report on the issue of municipal surveillance bylaws generally and made recommendations, in relation to FIPPA and the *Community Charter*, specific to pawnshop and second-hand dealer bylaws:

> In the case of bylaws dealing with pawnbrokers and second-hand dealers, we acknowledge that there is a public interest in preventing the fencing of stolen goods and in recovering stolen property. As noted earlier, the Pawnbrokers Association does not object to bylaws that require pawnbrokers to keep registers of property that they take in pawn and sell, but does not believe local governments have the power to force businesses to provide customer information to police agencies on a regular basis (as opposed to an item-by-item basis on inquiry by the police).
>
> Like the Pawnbrokers Association, the OIPC recognizes and supports the role of law enforcement agencies in ensuring that property left with such businesses is not stolen. Municipalities should not, however, be passing bylaws that place all citizens who do business with pawnbrokers or second-hand dealers under surveillance in the form of routine disclosures

[56] http://www.xtract.ca/pawnseconhanddealers.htm.
[57] *Royal City Jewellers & Loans Ltd. v. New Westminster (City)*, 2007 BCCA 398, [2007] B.C.J. No. 1661.

> of personal information of all customers. This is especially important because the Court of Appeal has yet to resolve doubt about whether s. 59(1)(b) of the *Community Charter* actually authorizes bylaws that compel collection and sharing of personal information in this way.[58]
>
> Specifically, we strongly believe that municipal bylaws regulating pawnbrokers and second-hand dealers should go no further than to require them to collect identifying personal information of those who leave goods and make that information available to police upon request in relation to specific stolen goods. Such a bylaw would require businesses to collect and retain identifying information. The only information that would be regularly disclosed would be information identifying goods pawned or sold. If goods were matched with stolen property, the personal information of the individual involved would be disclosed by paper or electronic means. This workable compromise may not satisfy all law enforcement officials, but it is a reasonable and justified position, particularly in light of the real and pressing dangers associated with the growth of surveillance databases and systems in our society.[59]

[125] The OIPC opposes any amendments to PIPA to address the issues that Xtract has raised and takes the position that no amendments should be made to the *Community Charter* that go beyond what the above passage contemplates.

6.9 NAID Canada

[126] The National Association for Information Destruction (Canada) ("NAID") is an organization that seeks to raise awareness and understanding of the importance of secure information and document destruction. It also plays an active role in developing and implementing industry standards and certification and provides a range of services to its members.

[127] The only specific recommendation contained in NAID's submission to the Committee is that PIPA should be amended to include a definition of information destruction. According to NAID, the safe destruction of personal information is so important to privacy protection that "it simply cannot be left to interpretation".[60] NAID has acknowledged that s. 35(2) of PIPA already requires organizations to destroy records containing personal information to documents when required under that section, but it believes that this obligation must be "backed up with an actual definition of destruction". NAID has suggested that "destruction" should be defined as "the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information (or parts thereof) is not practical."[61]

---

[58] After this report was published, the Court of Appeal struck down the City of New Westminster bylaw referred to here. See *Royal City Jewellers Ltd.*, cited above.
[59] *Local Governments & the Growth of Surveillance* (August 2006), at p. 10. www.oipc.bc.ca/publications/SurveillanceBylawDiscussionPaper.pdf.
[60] NAID submission, p. 4.
[61] NAID submission, p. 4.

[128] The OIPC is not persuaded such a definition is necessary and notes that NAID's proposed definition may be too narrow. The existing s. 35(2) requirement to destroy personal information is technology-neutral and can evolve as technologies of information destruction (and reconstitution) evolve. The OIPC notes that the legislative review of PIPEDA resulted in a recommendation for a definition of "destruction",[62] but the Alberta PIPA review did not.

6.10 Mutual Fund Dealers Association of Canada

[129] The Mutual Fund Dealers Association of Canada ("MFDA") is the national self-regulatory organization ("SRO") for the distribution side of the mutual fund industry.[63] The MFDA has been recognized by the British Columbia Securities Commission, for the purposes of the *Securities Act*, as an SRO.

[130] The MFDA's submission indicated that it has encountered situations where clients of mutual fund dealers attempt to revoke their consent to disclosure of their personal information to the MFDA where the client may be acting jointly with a member of MFDA in activity that the MFDA is investigating. The MFDA is concerned that, in such cases, a member of the MFDA may be shielded from investigation where the client, who is colluding with the MFDA member, withdraws consent to disclosure of personal information to the MFDA.

[131] The MFDA also has expressed concern that it may, because of PIPA, encounter difficulty obtaining personal information from third parties for investigation purposes, at least without a court order.[64]

[132] Accordingly, the MFDA has asked the Committee to recommend that s. 18(1)(j) of PIPA be amended to expand the list of qualified recipients of personal information in relation to investigations of possible violations of law. The MFDA has also expressed concern that its rules, regardless of their force because of the MFDA's status of an SRO, may not qualify as "laws of Canada or a province", as required under s. 18(1)(j).

[133] In view of the MFDA's law enforcement role, the OIPC does not object to the MFDA's proposed amendment, but believes that, rather than expressly referring to the British Columbia Securities Commission, it would be better to refer to a regulatory organization prescribed in regulations under PIPA. This would offer flexibility in designation of SROs.

[62] Recommendation 3.
[63] MFDA submission, p. 1.
[64] MFDA submission, p. 3.

6.11 BC Cancer Agency

[134] The BC Cancer Agency is a component of the Provincial Health Services Authority, a public body under FIPPA. The submission of the BC Cancer Agency expressed concern about s. 21(1)(b) of PIPA, which prohibits disclosure of personal information if it will be used to contact persons to ask them to participate in research. The BC Cancer Agency's submission noted similar concerns respecting s. 35(a.1) of FIPPA. It said that these provisions have had "the unanticipated effect of preventing or holding up key health research in the public interest."[65]

[135] The Commissioner is on record as having been opposed to enactment of s. 35(a.1) and has the same concerns respecting s. 21(1)(b). The OIPC recognizes that there is a need to protect privacy in relation to respecting disclosure of patients' personal information for the purpose of asking them to participate in research. The OIPC continues to be concerned, consistent with the Commissioner's statements in recent years, that these provisions in PIPA and FIPPA inappropriately impede research and should be replaced with a more balanced approach.

Recommendation 9––Section 21(1)(b) of PIPA should be replaced with a provision that appropriately protects the privacy of patients respecting contact for participation in research while facilitating the recruitment of individuals to participate in research.

7.0 Conclusion

[136] As noted in the Commissioner's preface, the OIPC is not recommending any change in direction for PIPA. As the clear majority of the submissions to the Committee illustrate, PIPA is a balanced law that requires no radical fix or overhaul. The OIPC's goal in making the above recommendations to the Committee is to improve the interpretation and application of the law for organizations, individuals and our office.

[137] As was also noted in the preface, it is important to ensure, to the extent possible, the ongoing substantial similarity of PIPA with PIPEDA and harmonization of PIPA with Alberta PIPA. The OIPC therefore asks the Committee to keep in mind the outcomes of the recent reviews by legislators of those laws.

[65] BC Cancer Agency submission, p. 1.

8.0 Summary of Recommendations

1. ***Recommendation 1––PIPA should be amended to include an express duty for organizations to notify affected individuals of unauthorized disclosure or use of their personal information, but the amendment should be carefully crafted so as to be effective, not over-broad. To that end, the amendment should address the following considerations:***

   (a) the kinds of personal information that must be involved before notice may be required, with personal information that is likely to create risks of financial loss or fraud being a key consideration;

   (b) who must be notified (affected individuals and the OIPC, with a possible added requirement to notify credit reporting agencies or law enforcement agencies in cases where financial loss is a risk);

   (c) how notice is to be given;

   (d) the timing of the giving of notice;

   (e) the general content of notices; and

   (f) authority for the Commissioner to order an organization to notify affected individuals of a privacy breach, on conditions the Commissioner may specify, where the organization has not given notice and the Commissioner considers that PIPA requires it.

2. ***Recommendation 2––The provisions of PIPA dealing with solicitor-client privilege, including the provisions empowering the Commissioner to examine records claimed to be privileged, should not be amended. Nor is any amendment necessary to protect the privilege.***

3. ***Recommendation 3––PIPA should be amended to permit non-consensual use and disclosure of "employee personal information" after termination of the employment relationship. The amendment should be carefully tailored to limit it to situations where the use or disclosure is necessary to manage post-employment relations or dealings between the employer and former employee.***

4. ***Recommendation 4––PIPA should be amended to make the complaint and review processes into a unitary process of the same nature as that recommended in 2004 by the Special Committee to Review the Freedom of Information and Protection of Privacy Act. The PIPA amendments should proceed hand in hand, as quickly as possible, with the comparable FIPPA amendments recommended in 2004.***

5. ***Recommendation 5––To provide clarity, s. 4 of PIPA should be amended, consistent with PIPEDA, to state that:***

(a) organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and

(b) organizations must use contractual or other means to ensure compliance with PIPA, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization.

6. ***Recommendation 6––Section 20 of PIPA should be amended to provide that an organization may disclose or collect personal information in its custody or under its control (including personal information about its employees, customers, directors, officers or shareholders) without consent as otherwise provided by s. 20.***

7. ***Recommendation 7––PIPA should be amended, in order to provide greater clarity for individuals and organizations, to give the Commissioner discretion to decline to open a complaint investigation or to dismiss a complaint if the Commissioner is satisfied that one or more of the following applies:***

(a) the request for review is not within the jurisdiction of the Commissioner;

(b) the request for review was not delivered within an applicable time limit;

(c) the request for review is frivolous, vexatious or trivial or gives rise to an abuse of process;

(d) the request for review was made in bad faith or for an improper purpose or motive;

(e) the person that asked for the review failed to diligently pursue the review or failed to comply with an order or direction of the commissioner in relation to it;

(f) there is no reasonable prospect the request for review will succeed;

(g) the subject matter of the request for review could be or has been appropriately dealt with in another proceeding or process;

(h) a fair and reasonable remedy or resolution to all or part of the request for review has been

(i) provided or made available by the public body to the person that asked for the review, and

(ii) the person that asked for the review has failed to accept the remedy or resolution;

(i) no meaningful remedy is available under the Act.

8. ***Recommendation 8––Section 32(2) of PIPA should be amended to permit organizations to charge a "reasonable fee" for access by an individual to her or his own personal information.***

9. ***Recommendation 9––Section 21(1)(b) of PIPA should be replaced with a provision that appropriately protects the privacy of patients respecting contact for participation in research while facilitating the recruitment of individuals to participate in research.***

APPENDIX

Draft Statutory Provisions

This appendix sets out draft amendments to the *Freedom of Information and Protection of Privacy Act* ("FIPPA") that the Commissioner proposed to the provincial government in 2005 in order to implement changes to that Act recommended in 2004 by the Special Committee to Review the Freedom of Information and Protection of Privacy Act. As set out above in the OIPC's submission respecting PIPA, the OIPC believes Parts 10 and 11 of PIPA should be repealed and replaced with a streamlined, unified set of provisions as close as to the following as practicable. Amendments to Part 5 of FIPPA and Parts 10 and 11 of PIPA ideally should proceed together.

Part 5 — Investigations, Audits and Reviews

Division 1 — Investigations, Audits and Reviews by the Commissioner

Authority for investigations, audits or reviews

52(1) The commissioner may conduct an investigation or audit to monitor how the Act is administered and to ensure compliance with any of its provisions, and, for this purpose, may make

(a) a report, including findings and recommendations, or

(b) an order under section 58.

(2) The commissioner may conduct a review:

(a) if asked by an applicant that made a request for access to a record to the head of a public body, other than the commissioner or the registrar under the *Lobbyist Registration Act*, to review a decision, act or failure to act of the head in relation to that request,

(b) if asked by a third party notified under section 24 of a decision to give access to a record by the head of a public body, other than the commissioner or the registrar under the *Lobbyist Registration Act*, to review any decision made about the request by the head of the public body.

(c) if asked by an individual to review whether a public body or service provider has failed to comply with Part 3 of the Act in relation to the individual's personal information,

(d) if asked by the head of a public body, to authorize the public body to disregard requests under section 5 or 29 that

(i) would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the request, or

(ii) are frivolous, vexatious or trivial or give rise to an abuse of process.

How to ask for a review

53(1) To ask for a review under this Division, a written request must be delivered to the commissioner.

(2) A request for a review of a decision of the head of a public body must be delivered within

(a) 30 days after the person that asked for the review is notified of the decision, or

(b) a longer period allowed by the commissioner.

(3) The failure of the head of a public body to respond in time to a request for access to a record is to be treated as a decision to refuse access to the record, but the time limit in subsection (2) (a) for delivering a request for review does not apply.

Notifying others of review

54(1) On receiving a request for a review under section 52(2)(a) to (c), the commissioner must give a copy to

(a) the head of the public body concerned, and

(b) any other person that the commissioner considers appropriate.

(2) On receiving a request for review under section 52(2)(d), the commissioner must give a copy to

(a) the applicant that made the request under section 5 or 29, and

(b) any other person that the commissioner considers appropriate.

Settlement and summary resolution of a review

55(1) The commissioner may at any time do one or more of the following:

(a) decline to proceed with all or part of a review if the person that asked for the review does not present sufficient information or a reasonable basis to identify a reviewable matter under section 52(2);

(b) direct the person that asked for the review to pursue resolution of all or part of the subject matter of the review through informal means or alternative processes and remedies;

(c) make an order dismissing summarily all or part of the review in accordance with section 55.1; or

(d) appoint a person to consider and assist the parties to settle or otherwise resolve all or part of the subject matter of the review.

(2) A person appointed under subsection 1(d) may exercise the commissioner's powers for conducting a review but must not decide the merits of the review unless the parties consent.

Summary dismissal of a review

55.1(1) In making an order under section 55(1)(c), the commissioner must be satisfied that one or more of the following apply:

(a) the request for review is not within the jurisdiction of the commissioner;

(b) the request for review was not delivered within an applicable time limit;

(c) the request for review is frivolous, vexatious or trivial or gives rise to an abuse of process;

(d) the request for review was made in bad faith or for an improper purpose or motive;

(e) the person that asked for the review failed to diligently pursue the review or failed to comply with an order or direction of the commissioner in relation to it;

(f) there is no reasonable prospect the request for review will succeed;

(g) the subject matter of the request for review could be or has been appropriately dealt with in another proceeding or process;

(h) a fair and reasonable remedy or resolution to all or part of the request for review has been

(i) provided or made available by the public body to the person that asked for the review, and

(ii) the person that asked for the review has failed to accept the remedy or resolution;

(i) no meaningful remedy is available under the Act.

(2) Before dismissing all or part of a review under subsection (1), the commissioner must give an opportunity to be heard to the person that asked for the review and to any person notified under section 54.

(3) If the commissioner dismisses all or part of a review under subsection (1), the commissioner must give a copy of the decision and the reasons for it to the person that asked for the review and to any person notified under section 54.

Conduct of investigation, audit or review

55.2(1) Subject to this Act, the commissioner has the power to control his own processes and may make rules respecting practice and procedure for conducting an investigation, audit or review.

(2) The commissioner may receive evidence and other information on oath, affidavit or in any other manner, whether or not it would be admissible in a court of law;

(3) The commissioner may conduct all or part of an investigation, audit or review in private.

(4) The commissioner may decide whether representations are to be made orally, in writing or by electronic means;

(5) The commissioner may determine whether a person is entitled to be present or to comment on representations made to the commissioner by another person.

(6) The commissioner may at any time make an order requiring a person:

(a) to attend an oral or electronic hearing to give evidence on oath, affirmation or in any other manner;

(b) to produce for the commissioner a record in the person's custody or control, as specified by the commissioner.

(7) The commissioner may enter any premises occupied by a public body or service provider and examine any records found in those premises.

(8) The commissioner may apply to the court for an order

(a) directing a person to comply with an order made by the commissioner under subsection (6),

(b) directing a public body or any director or officer of a person to cause the person to comply with an order made by the commissioner under subsection (6),

(c) authorizing the commissioner to enter premises and examine records under subsection (7).

(9) The commissioner may examine any information in a record, including personal information and information that is subject to solicitor client privilege.

(10) If a person discloses a record that is subject to solicitor client privilege to the commissioner at the request of the commissioner, or under subsections (4) to (7), the solicitor client privilege of the record is not affected by the disclosure.

(11) Despite any other enactment or legal privilege, a public body must produce to the commissioner within 10 days any record or a copy of any record required under this section.

(12) If a public body is required to produce a record under subsection (4)(b) and it is not practicable to make a copy of the record, the head of the public body may require the commissioner to examine the original at its site.

(13) After completing an investigation, audit or review, the commissioner must return any record or any copy of any record produced by a public body concerned unless an application for judicial review or an appeal from a decision with respect to that application is filed.

Conduct of investigation or audit

55.3 In addition to powers under section 55.2 and before making an order directed to a public body or service provider, the commissioner, in conducting an investigation or audit, must give an opportunity to be heard to the public body or service provider concerned and to any other person that the commissioner considers appropriate.

Conduct of review

55.4(1) In addition to powers under section 55.2, the commissioner, in conducting a review, must give an opportunity to be heard to the person that asked for the review and to any other person notified under section 54.

(2) The commissioner may allow a person to intervene in a review if the commissioner is satisfied that:

(a) the person can make a valuable contribution or bring a valuable perspective to the review, and

(b) the potential benefits of the intervention outweigh any prejudice caused by the intervention to the person that asked for the review or to any other person notified under section 54.

(3) The commissioner may impose terms and conditions on the participation of an intervener.

(4) A review must be completed within 90 days after receiving the request for review unless the commissioner

(a) specifies a later date, and

(b) notifies all of the participants in the review.

(5) The calculation of the 90-day time referred to in subsection (4) does not include any period for resolution of all or part of the review under section 55(1)(b).

Statements made to the commissioner not admissible in evidence

56.1(1) A statement made or an answer given by a person during an investigation, audit or review is inadmissible in evidence in court or in any other proceeding, except in

(a) a criminal proceeding,

(b) a prosecution for an offence under this Act, or

(c) an application for judicial review or an appeal from a decision with respect to that application.

(2) Subsection (1) applies also in respect of evidence of the existence of proceedings conducted before the commissioner.

Protection against libel or slander actions

56.2 Anything said, any information supplied or any record produced by a person during an investigation, audit or review is privileged in the same manner as if the investigation, audit or review were a proceeding in a court.

Compulsion protection

56.3(1) The commissioner or a person acting on behalf of or under the direction of the commissioner must not be required to testify or produce evidence in any proceeding, other than a criminal proceeding, about records or information obtained in conducting an investigation, audit or review under this Act.

(2) Despite subsection (1), the court may require the commissioner to produce the record of a review proceeding that is the subject of an application for judicial review under the *Judicial Review Procedure Act*.

Burden of proof for decision to give or refuse access

57(1) At a review into a decision to refuse an applicant access to all or part of a record, it is up to the head of the public body to prove that the applicant has no right of access to the record or part.

(2) However, if the record or part that the applicant is refused access to contains personal information about a third party, it is up to the applicant to prove that disclosure of the information would not be an unreasonable invasion of the third party's personal privacy.

(3) At a review into a decision to give an applicant access to all or part of a record containing information that relates to a third party,

(a) in the case of personal information, it is up to the applicant to prove that disclosure of the information would not be an unreasonable invasion of the third party's personal privacy, and

(b) in any other case, it is up to the third party to prove that the applicant has no right of access to the record or part.

Commissioner's orders

58(1) On completing an investigation, audit or review, the commissioner may dispose of the issues by making an order under this section.

(2) For a review into a decision of the head of a public body to give or to refuse to give access to all or part of a record, the commissioner must, by order, do one or more of the following:

(a) require the head to give the applicant access to all or part of the record, if the commissioner determines that the head is not authorized or required to refuse access;

(b) either confirm the decision of the head or require the head to reconsider it, if the commissioner determines that the head is authorized to refuse access;

(c) require the head to refuse access to all or part of the record, if the commissioner determines that the head is required to refuse access;

(d) require the head to comply with section 4(2).

(3) For an investigation, audit or review into any other matter, the commissioner may, by order, do one or more of the following:

(a) confirm that a duty imposed by this Act or the regulations has been performed or require that a duty imposed by this Act or the regulations be performed;

(b) confirm or reduce the extension of a time limit under section 10;

(c) confirm, excuse or reduce a fee, or order a refund, in the appropriate circumstances, including if a time limit is not met;

(d) confirm a decision not to correct personal information or specify how personal information is to be corrected;

(e) require a public body or service provider to stop collecting, using or disclosing personal information in contravention of this Act, or confirm a decision of a public body or service provider to collect, use or disclose personal information;

(e.1) authorize the public body to disregard requests under section 5 or 29 that

(i) would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the request, or

(ii) are frivolous, vexatious or trivial or give rise to an abuse of process.

(f) require the head of a public body to destroy personal information collected in contravention of this Act.

(4) The commissioner may specify any terms or conditions in an order made under this Act.

(5) The commissioner must give a copy of an order made under this section to the parties and interveners that participated in the review and the minister responsible for this Act.

Duty to comply with orders

59(1) Not later than 30 days after being given a copy of an order of the commissioner under section 58, the head of the public body concerned or any service provider to whom the order is directed, as applicable, must comply with the order unless an application for judicial review of the order is brought before that period ends.

(2) If an application for judicial review is brought before the end of the period referred to in subsection (1), the order of the commissioner is stayed for 90 days from the date the application is brought, subject to any additional conditions ordered by the court.

Enforcement of orders

59.01(1) The commissioner or a person in whose favour the commissioner makes all or part of an order may file a certified copy of the order with the court.

(2) An order filed under subsection (1) has the same force and effect, and all proceedings may be taken on it, as if it were a judgment of the court.

* * *