



Statutory Review of the *Personal Information Protection Act*

General Briefing for the Special Committee to Review the *Personal Information Protection Act*

May 29, 2007

David Loukidelis  
Information & Privacy Commissioner for British Columbia

## **TABLE OF CONTENTS**

	<b><u>Page</u></b>
<b>1. INTRODUCTION</b>	<b>3</b>
<b>2. ROLE &amp; MANDATE OF THE OIPC</b>	<b>3</b>
<b>3. WHY IS PRIVACY IMPORTANT?</b>	<b>4</b>
<b>4. THE BASIC RULES OF PRIVATE SECTOR PRIVACY</b>	<b>6</b>
<b>5. SELECTED ISSUES</b>	<b>8</b>
<b>6. SNAPSHOTS OF IPA</b>	<b>9</b>
<b>6.1 Case Summaries: PIPA Complaints</b>	<b>10</b>
<b>6.2 Case Summaries: PIPA Requests for Review</b>	<b>21</b>
<b>6.3 Case Summaries: PIPA Orders</b>	<b>23</b>

## 1. INTRODUCTION

British Columbia's *Personal Information Protection Act* ("PIPA") came into force on January 1, 2004. This brought British Columbia into line with the rest of Canada, and with most jurisdictions in the industrialized world, in regulating the privacy practices of private sector organizations.

Because of its importance, and because it is a new kind of legislation in British Columbia, the Legislature provided in PIPA that the law must be reviewed periodically by an all-party special committee of the Legislative Assembly. On April 19, 2007, the Legislative Assembly by resolution created the Special Committee to Review the Personal Information Protection Act. A similar legislative review is under way respecting Alberta's *Personal Information Protection Act*<sup>1</sup> and a committee of Parliament last week tabled a report on its review of the federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act*<sup>2</sup>.

This document provides the committee with a general outline of the information privacy concepts that underpin PIPA. It also offers a general overview of PIPA and the experience to date of the Office of the Information and Privacy Commissioner ("OIPC") in overseeing compliance with PIPA.

The OIPC recommends that the committee hold public hearings and invite written submissions in order to hear from an array of stakeholders. The OIPC has already provided the committee with a list of several dozen stakeholders that the committee may wish to consult. For its part, the OIPC will supplement this general briefing with a formal submission to the committee at a later date.

## 2. ROLE AND MANDATE OF THE OIPC

Before proceeding with the PIPA overview, a few words about the OIPC will help explain its interest in this review.

The Information and Privacy Commissioner is an independent officer of the Legislature. The OIPC was established in 1993 to provide independent review of access to information decisions made by the more than 2,000 public bodies that are covered by the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). FIPPA restricts the collection, use and disclosure of personal information by public bodies and the OIPC investigates complaints that public bodies have failed to comply with these privacy protection provisions.

The OIPC also oversees compliance with PIPA, which covers more than 300,000 for-profit and not-for-profit private sector organizations, including businesses,

---

<sup>1</sup> <http://www.assembly.ab.ca/PIPARReview/default.htm>.

<sup>2</sup> [http://www.oipc.bc.ca/sector\\_private/public\\_info/391\\_ETHI\\_Rpt04\\_PDF-e.pdf](http://www.oipc.bc.ca/sector_private/public_info/391_ETHI_Rpt04_PDF-e.pdf).

---

charities, religious organizations, associations, trade unions and trusts. PIPA contains rules about organizations' collection, use and disclosure of individuals' personal information. 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.

### **3. WHY IS PRIVACY IMPORTANT?**

One privacy expert has said this about the importance of privacy<sup>3</sup>:

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.

The term "privacy" is not actually defined in British Columbia legislation and privacy can mean different things to different people.

To some, privacy means the "right to be let alone". To others, it means anonymity. Still others believe it means the right to be unobserved. Under PIPA, privacy means maximizing, wherever possible and to the extent that is reasonable, a citizen's control over the collection, use and disclosure of his or her personal information.

---

<sup>3</sup> Simon Davies, *Big Brother: Britain's Web of Surveillance & the New Technological Order* (London: Pan, 1996).

PIPA is essentially a privacy roadmap. It contains a set of internationally recognized rules—called “fair information practices”—that govern the collection, use and disclosure of personal information. Modern privacy principles and legislation emerged in the late 1960s, when the Council of Europe began studying the effect of computer technology on personal privacy. The first European data protection laws was enacted in the early 1970s. In 1980, the Organization for Economic Co-operation and Development (OECD) developed its *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, commonly referred to as the OECD Guidelines. In 1995, the European Union passed a Directive on data protection, a legal instrument that binds all member states. Among other things, the EU Directive prohibits the electronic export of personal data to any country that does not have an adequate level of legal privacy protections.

Many state and federal privacy laws exist in the United States. Examples of federal laws affecting the private sector include the Gramm-Leach-Bliley Act of 1999 (financial privacy), the health privacy regulations under the *Health Insurance Portability and Accountability Act* and the *Children’s Online Privacy Protection Act*. The number and variety of privacy-related laws in the United States is growing rapidly, with recent developments focussing on identity theft and notification of consumers whose personal information has been compromised.

In Canada, the first privacy commissioner was established under the 1977 *Human Rights Act* and in 1982 the first privacy commissioner was appointed under the new federal *Privacy Act*. Quebec passed its first privacy law in 1982, with Ontario following in 1987. As with access to information, all provinces and territories now have public sector privacy laws.

Private sector privacy laws first emerged in Canada with Quebec’s enactment in 1994 of privacy rules for the private sector. Parliament later enacted the *Personal Information Protection and Electronic Documents Act*, which came into force in stages, beginning in 2001, and British Columbia and Alberta followed suit.

PIPA came into force on January 1, 2004. Section 2 of PIPA states its purposes:

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.

PIPA applies to “personal information”, which it defines as information about an “identifiable individual”. PIPA does not apply to “business contact information” or “work product information”, terms defined in the law.

PIPA also 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).

#### **4. THE BASIC RULES OF PRIVATE SECTOR PRIVACY**

PIPA sets out requirements for how organizations may collect, use, disclose and secure personal information. The rules, which are consistent with international standards, are summarized below.

##### *Consent for collection of personal information*

Organizations must obtain consent for collecting, using and disclosing an individual's personal information, except where PIPA excuses consent (including respecting employee personal information reasonably needed for the employment relationship, collection in an emergency and collection for an investigation where consent would compromise the availability or accuracy of the information). Consent must be obtained in a form appropriate to the sensitivity of the personal information. If an individual modifies or withdraws consent, an organization must comply with the change. If an individual wants to withdraw consent, an organization must explain the consequences of withdrawal.

##### *Limits on collection of personal information*

Organizations must collect personal information only for reasonable purposes and must collect only as much as is reasonable for those purposes. PIPA repeatedly refers to what "a reasonable person would consider appropriate in the circumstances." Unless PIPA allows it, organizations must collect personal information directly from the individual concerned and tell the individual how they intend to use and disclose the information at or before the time the information is collected.

##### *Use and disclosure of personal information*

Organizations must use and disclose personal information only for the purpose for which it was collected, unless the individual consents or PIPA permits the new use or disclosure without consent.

##### *Access to personal information*

On request, an organization must provide an individual with information about the existence, use and disclosure of the individual's personal information and provide access to that information unless PIPA excuses the organization from giving access in whole or in part. Also on request, and where satisfied on reasonable

---

grounds, an organization must correct information that is inaccurate or incomplete. Organizations may charge a minimal fee for responding to a request for access, but the fee should not be a barrier to access.

#### *Accurate and complete personal information*

An organization must ensure that personal information it has collected is as accurate and complete as necessary for the purpose it is to be used for and ensure it is secure. An organization can keep personal information for only as long as reasonable for business or legal reasons.

#### *Designating a Privacy Officer*

An organization must designate someone who is responsible to ensure the organization complies with the law.

#### *Policies & Procedures*

An organization must develop policies and procedures necessary for it to meet its obligations under PIPA, as well as a complaint process respecting the application of PIPA, and make these available on request.

#### *Resolution of Complaints*

An organization must create mechanisms for resolving in a fair and timely fashion complaints about the collection, use and disclosure of personal information.

#### *Special Rules for Employment Relationships*

Under PIPA, an employee is someone employed by the organization or someone who performs a service for the organization and includes an apprentice, a volunteer and a work experience or co-op student.

Under PIPA, “employee personal information” is a distinct category of personal information. It refers to personal information that is reasonably needed to establish, manage or end an employment relationship. It does not include personal information about employees held by an organization that is not related to those things.

Personal information does not include business “contact information”, which is an individual’s name and position or title, business telephone number, business address, business e-mail, business fax number and other business contact information. It also does not include “work product information”, which is information prepared by individuals or employees in the context of their work or business. The “work product” designation applies only from the perspective of the individual who created the record. One employee’s work product may include

personal information of another individual. For example, an employee performance report prepared by a management employee of a company would be work product information as it relates to that management employee, but the personal information about the employee being assessed would be the personal information of the other employee.

Organizations are not required to seek consent from employees for the collection, use and disclosure of employee personal information, provided the information is collected for the purpose of establishing, managing or terminating the employment relationship. They are required to give their employees prior notice that they are collecting, using or disclosing the information and the purposes for doing so.

## **5. SELECTED ISSUES**

The case summaries found in part 6, below, illustrate the range of issues with which the OIPC deals under PIPA. This section highlights a recently prominent issue—that of information security and privacy breaches. Losses of personal information, or inappropriate browsing of personal information, are often in the news these days and the OIPC has been very active in this field.

Our activities regarding privacy breaches aim to promote common sense good privacy practices. Our activities also seek to assist organizations to meet their obligation under PIPA to protect personal information in their custody and control by making reasonable security arrangements to prevent risks such as unauthorized access, collection, use or disclosure. Organizations must, therefore, take suitable steps to protect against privacy breaches and to react appropriately should a privacy breach occur.

A privacy breach occurs when there is unauthorized collection, use, disclosure or disposal of personal information. Such activity is “unauthorized” if it occurs in contravention of PIPA. The most common privacy breach happens when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed.

Of the 34 breach notifications the OIPC received in 2005-06, 12 were related to PIPA.

The most common privacy breaches resulted from theft. Thieves stole everything from computers to backpacks and bins of paper set out for shredding. In every case, the organization had failed to properly secure the personal information to prevent access in the event of theft. A second common example of a privacy breach was loss of records by courier companies. In one case, the driver left the vehicle running and unlocked during a delivery. The vehicle was stolen with medical files in it. Less common, but still persistent, were reports of

misuse of personal information by employees. Generally, the cases involved accessing data base information regarding a particular third party for non-work related purposes.

Perhaps the most high profile types of privacy breaches are those related to inappropriate disposal—the cases of medical and legal files blowing down the street or the case of the sale of government computers with personal information still contained on the hard drives.

As a result of our investigations into the privacy breaches reported in 2005-06, the OIPC developed the following list of suggested safeguards that may assist in reducing the chances of a privacy breach. These are found on the OIPC's website ([www.oipc.bc.ca](http://www.oipc.bc.ca)):

- Faxing and Emailing Personal Information
- Protecting Personal Information Away from the Office
- Physicians and Security of Personal Information

During 2006, we also published a number of resources on how to respond to privacy breaches when they do occur:

- Key Steps in Responding to Privacy Breaches
- Privacy Breach Reporting Form (Updated Dec 2006)
- Breach Notification Assessment Tool
- Key Steps for Physicians in Responding to Privacy Breaches

## **6. SNAPSHOTS OF PIPA**

PIPA gives individuals the right to ask the OIPC to review matters where they are not satisfied with how an organization has

- responded to a request for personal information;
- responded to a request for correction of personal information;
- responded to a complaint about how it treats personal information; or
- followed or not followed any provision of PIPA.

A request for a review of an organization's decision, act or failure to act concerning a request for access to information or correction of personal information must be made to the OIPC within 30 business days after the organization's decision. A dispute concerning the collection, use and disclosure of personal information, fees or a dispute on any other matter is termed a "complaint". PIPA does not impose a time limit for making a complaint but, unless there are extenuating reasons, the OIPC will not generally entertain a complaint made more than six months after the individual concerned had notice of the circumstances.

---

The OIPC will generally defer or adjourn acting on a complaint or request for review 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.

Our approach to PIPA requests for review and complaints is similar to the approach we take to FIPPA complaints. We investigate the circumstances of the dispute, consider the application of relevant sections of PIPA to those circumstances and, where practicable, 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.

In 2005-06, the OIPC received 47 requests for review and 134 complaints under PIPA and closed 49 requests for review and 146 complaints. In 2006-2007, preliminary figures indicate that the OIPC received 103 complaints under PIPA and 59 requests for review.

Our early impression that the majority of enquiries and complaints under PIPA would involve smaller organizations has been borne out. Early on, we received more complaints against retail stores and insurance and financial institutions. Generally, these organizations or their umbrella trade groups had the resources to develop and refine their privacy policies and dispute resolution mechanisms. As time has gone on, they have been the source of a smaller proportion of the PIPA complaints we receive.

The largest volume of complaints and requests now are generated by employees of small businesses concerned about their employer's information practices or, more commonly, former employees seeking their own personal information. Employees in provinces covered by PIPEDA do not have the same level of legislative protection for their personal information. Employees of larger organizations frequently call this office for information about PIPA but are able to resolve their issues with their employer. Our "Guide to PIPA for Businesses and Organizations", a copy of which is provided along with this briefing document, was designed for small to medium sized businesses, as was our resource document entitled "PIPA and the Hiring Process: Frequently Asked Questions." (All of our resource materials are available on our web site at [www.oipc.bc.ca/](http://www.oipc.bc.ca/).)

Housing issues, including those involving strata corporations, housing cooperatives and residential tenancies, generate the next highest volume of enquiries and complaints. Perhaps, due to the nature of the housing market, residential tenancy issues generally come to us as enquiries—*i.e.*, requests for information—rather than as formal complaints. We are in the course of developing resource materials to assist landlords and tenants, and strata corporations, to ensure PIPA's obligations are met.

Professionals operating as small businesses also generate a significant proportion of our requests and complaints, most often concerning access requests and the fees assessed by these organizations for providing individuals with their own personal information. Particularly in the early days of PIPA, it was fairly common for these organizations to fail to respond to requests for personal information at all or in a timely manner, frequently because the organizations were simply not aware of their PIPA obligations. We focus our investigations and mediations on ensuring that these organizations become more familiar with PIPA and how to respond to access requests. If a dispute involves fees, we most often involve the relevant professional governing bodies and associations, which often set suggested fee schedules for their members. In this way, complaint resolutions can have a broader application within a profession. As experience with PIPA has matured, these kinds of complaints have decreased in number somewhat.

## **6.1 Case Summaries: PIPA Complaints**

To give some sense of the range of complaints that the OIPC investigates, the following selected case summaries illustrate generally the kinds of complaints that the OIPC receives.

### **Second Rule for Obtaining Consent—Get It If the Law Requires It**

At a labour relations hearing, a former employer told a worker that he had contacted other previous employers to obtain personal information about the worker. The worker wrote to the former employer asking him what he had collected and for what purpose. The former employer did not fully respond and the worker asked us to investigate.

Our investigation revealed that the employer had contacted one other previous employer but had received no information. There was technically no breach of PIPA because no personal information had been collected or disclosed. However, we informed the former employer that he could not collect personal information about previous employees without their consent. PIPA describes circumstances in which an individual is deemed to consent to the collection of information (section 8) and in which personal information can be collected without consent (section 12), but the circumstance about which the worker complained did not fall into either category. (The “Guide for Businesses and Organizations to BC’s PIPA”<sup>4</sup> and “PIPA and the Hiring Process”<sup>5</sup> on our website provide more information in this area.)

---

<sup>4</sup> [http://www.oipc.bc.ca/pdfs/private/a- GUIDE TO PIPA\(3rd ed\).pdf](http://www.oipc.bc.ca/pdfs/private/a- GUIDE TO PIPA(3rd ed).pdf).

<sup>5</sup> [http://www.oipc.bc.ca/pdfs/private/PIPAHiringFAQ\(10APR06\).pdf](http://www.oipc.bc.ca/pdfs/private/PIPAHiringFAQ(10APR06).pdf).

---

### **Employer Ignores Former Worker's Request for Record of Hours Worked**

A former employee of a dental office made a request under section 23 of the *Personal Information Protection Act* for copies of any records containing her personal information. After the dental office responded, she wrote back to say that she hadn't received a record of the hours she had worked each day. She asked for access to the ledger recording that information, emphasizing that she had no interest in obtaining the personal information of other staff. When the dental office denied the request, the woman asked our office to review that decision.

The dental office told us they had refused to release the information in the ledger because the woman already had all her payroll information on her payslips. However, they confirmed that the ledger contained the daily record of the hours worked by the applicant. We explained that, regardless of what the pay slips contained, the details of the hours worked were the former employee's personal information and should be released to her if the personal information of other staff could first be removed. The contact agreed to bring this up for discussion with the dentists at the office.

After agreeing to release a severed version of the ledger entries, the dental office sent it to us and asked us to send the record to the applicant. It is not our practice to release records on behalf of public bodies or private sector organizations, so we asked the dental office to send the woman the record themselves. We also noted that many of the severed ledger pages did not include the individual entry dates, and the dental office contact agreed to make sure they were complete. In due course the applicant received the withheld records and the matter was resolved.

### **Club Protests Misuse of Membership List**

A private club complained that the trade union representing club members had used the club's membership list, which contained the names and telephone numbers of each of the club members, to compile a mailing list from which it sent two mailings to the club members to solicit their support in a labour dispute.

The trade union refused to respond to the club's questions about how it collected and used club members' personal information. However, after we reminded the trade union of its obligations under PIPA, it agreed to respond to the club's questions. It also agreed to purge the club membership information from its internal computer system and to ensure that all hard copies of the information were destroyed.

---

## **Condo Owners at Odds Over Security Video System**

The strata council for a condominium development had received many complaints from residents about crime and vandalism, deteriorating levels of personal safety and a general decline in the livability of the development as a result of drug users, sex trade workers and petty criminals using parts of the building, its entrances and its covered parking. The council chose to have a security system installed at each of the entrances to the building and parking lot. The camera feeds were recorded to a computer hard drive in a locked utility room, which overwrote (recorded over) itself approximately every seven days. The live camera feeds were available to each resident (and only to residents) through a dedicated channel provided by the cable television supplier.

A number of residents were extremely unhappy about the recording of movements by residents and the live broadcast of these movements to other residents. They complained to the OIPC that the security system was collecting personal information without their consent, contrary to PIPA requirements.

In examining the matter, we found the complainants' allegations to be correct—their images were in fact being recorded and held over a rolling seven-day period and their images were being broadcast to building residents. At the same time, the strata council president argued that the overwhelming majority of residents endorsed the system and were grateful for the dramatic drop in vandalism, mischief and general intimidation since the system had been installed. In the final analysis, PIPA did not provide a solution to a situation where a majority of residents approved of the data collection and some did not. We wrote as follows:

...it would appear that a resolution of these concerns may be achieved with a measure of goodwill and continued discussion within the strata community at [address] as to how best to balance the benefits of the system with the perceived intrusiveness. For that, PIPA does not offer a definitive test other than that of "what a reasonable person would consider appropriate in the circumstances."

We closed the letter with a series of recommendations to the strata council concerning warning signage for the video surveillance system, developing a written policy and appointing a privacy officer and, at the strata corporation annual general meeting, revisiting the status of the system as an acceptable measure. We made a tentative finding of "partially substantiated" and advised that we could examine the issue again in the event of subsequent complaints.

## **Sporting Body Gets Up to Speed on PIPA Responsibilities**

A provincial sporting association investigated a complaint about the behaviour of one of its members and followed up with disciplinary action. When the member's lawyer wrote to the association requesting copies of records resulting from the disciplinary proceedings, the association acknowledged that the disciplinary

proceedings were complete but did not respond to the request for records. The lawyer asked us to review the association's failure to respond.

When we contacted the association, it became apparent that its staff had vaguely heard of the *Personal Information Protection Act* but were not familiar with its details or how the law applied to their organization. We explained how PIPA applies to the access request made on behalf of the affected individual. We explained that an organization must, within 30 business days, respond to a request by an applicant for access to his or her personal information. We also explained that, if access to all or part of the requested information is denied, the organization must tell the applicant why, with reference to the provisions of PIPA on which the refusal is based. We told the organization that PIPA also requires an organization to provide the name and contact information of someone in the organization who can answer questions about the refusal and to inform applicants that they have the right to request a review, within 30 days of being notified of the refusal, of the organization's response by the OIPC.

The association agreed to write another response letter that would fulfil its obligations under PIPA. The applicant's lawyer confirmed receiving the response letter and was satisfied with the association's response. No further action was required and our file was closed.

### **Housing Co-op Disclosures: Meeting Notices**

A member of a housing co-op ran afoul of other members following alleged misconduct on the premises by a family member. As a result, she faced an expulsion vote at a general meeting of the co-op membership. The co-op board posted a detailed notice of the pending vote meeting, and the reasons for it, in several public areas of the co-op property, including the recreation centre, which was accessible to guests of co-op members. The woman then complained to us that the quasi-public posting of information about her was contrary to PIPA and a defamatory invasion of her privacy, especially since the matters that would be decided had not yet been the subject of the membership's vote.

We found that the disclosure as effected by the board was permitted by PIPA section 18(o), but only to the extent that the disclosure is consistent with the law that requires or authorizes it, in this case the *Cooperative Association Act*. We recommended that the co-op board comply with PIPA by following its own rules and the *Cooperative Association Act*, requiring personal delivery of the notice to each member. Legal counsel for the co-op agreed and the practice of public posting of such notices stopped. On this basis, the complainant's concerns were resolved.

---

## **Too Sick To Work? Prove It**

What are the rights of an employer to request documentation from an employee to validate sick leave? We confronted this question in the context of PIPA when a person complained that her employer had made an unreasonable request for “relevant medical information” regarding her condition and her prognosis for returning to work. PIPA section 13(2)(b) allows collection of employee personal information without the employee’s consent, if it is “reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.”

In examining the matter, we concluded that PIPA, including the above test and a general requirement of “reasonableness”, imports a large part of the common law of employment.

Given the nature of the work, which required consistent attention to detail, and the nature of the medical issue, we concluded that the employer’s request was within the reasonable application of section 13 of PIPA. For that reason, we did not substantiate this complaint.

## **Personal Information Pops Up in Ad**

A core purpose of privacy legislation is to prevent deliberate or unintentional misuse of personal information. Unfortunately, mistakes happen even with the best of intentions, with or without a sound privacy policy. One of our common roles is to mend fences where mistakes have been made.

A professional wanted to find a trusted person to come to her house every day and take care of her baby boy while she was at work. She put a notice in a community newspaper looking for just such a person. Soon afterwards she moved and sent the newspaper her updated contact information for its records.

The next week, when the woman opened the newspaper on the date the notice first appeared, she was appalled to see that the notice included her home address. When she contacted the newspaper to express her outrage, the office manager apologized profusely, explaining that the information had been put in the paper by mistake. The office manager said that the person who made the mistake had been reprimanded and offered to run the corrected ad free of charge for several weeks.

Although the error had been small, the impact on the advertiser was significant. Understandably, she continued to feel vulnerable and nervous. She felt that the paper hadn’t gone far enough but she didn’t want to have any further direct dealings with it. She asked us for assistance in arriving at a resolution to ensure that there was as little risk as possible from the notice having been run.

After we acted as an intermediary between the woman and the paper, the office manager provided assurance that the erroneous ad had been erased from the computer file and had been blocked out of archived issues. In addition, we gave the newspaper suggestions about useful resources for developing a privacy policy, including guidance on our website.<sup>6</sup>

### **Client Files Vanish with Stolen Laptop**

A lawyer had his laptop computer stolen from his desk while he was at lunch and the office receptionist was away from her desk. The laptop contained previous and current client files and information relating to legal work he had completed for his clients, including contracts, notarized documents, leases and wills.

The lawyer immediately notified the police and the Law Society of British Columbia, the governing body for lawyers. The police told him it was very unlikely that he would recover his laptop but that the thief would likely wipe the hard drive to eliminate any information that would identify the previous owner. The Law Society did not plan further action.

The lawyer used our office's recently developed Privacy Breach Reporting Form (posted on our website) to report to us the loss of his clients' personal information. As suggested on the form, the lawyer had conducted an assessment of the risk of the loss of personal information to his clients and to his firm. Client billing information was kept separate from client legal files and the laptop contained only names and addresses of clients and legal documents. There was no client financial information on the laptop.

We suggested that the lawyer notify his current and former clients of the loss of their personal information. He did so by letter for those for whom he had current addresses and contacted others directly by telephone. Fewer than 10 of his clients called him about the breach. Their concerns were alleviated when they learned that only limited personal information was on the computer.

To guard against similar breaches in the future, the law firm changed its policies to ensure that the receptionist was always at the front of the office during business hours and that the front door would be locked if she had to step away from the front desk. The firm also ensured that both laptop and desktop computers would be locked to desks to deter theft.

We were satisfied that the lawyer and his law firm had taken the necessary steps to:

- contain the privacy breach and the risk of further breach;
- assess the risk to his clients of the loss of their personal information;
- notify his clients, and other relevant agencies, of the breach; and
- prevent future breaches of this nature.

---

<sup>6</sup> [http://www.oipc.bc.ca/sector\\_private/resources/privacy\\_policy.htm](http://www.oipc.bc.ca/sector_private/resources/privacy_policy.htm).

---

**Biometric Scan of Employees OK for Payroll Purposes in Some Circumstances....**

Demagnetization is a common failure of swipe cards used for monitoring actual time worked by employees. A hotel faced with this problem notified its employees that it would replace the swipe cards with a biometric scanning process. The process uses an image of an individual's finger to authenticate that the person who is entering or leaving the premises is that individual. It does not record the employee's fingerprint and therefore cannot later reproduce it. The system generates a number derived from measurements of various points of the subsurface of the employee's finger or thumb.

An employee brought his concerns to his manager and, when he felt his concerns were ignored, he requested our assistance. He said he considered the new system to be both an invasion of privacy and unnecessary, and argued that the employer hadn't explained why it was being implemented. He added he believed that requiring a thumbprint is invasive and wondered whether it was legal for the hotel to demand it, rather than providing an alternative option for employees to verify their identity and in and out times.

PIPA authorizes the collection, use and disclosure of employee personal information without the consent of the individual employee, if it is "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual." We took the position that balancing an employee's right to protect his or her personal information against the authorization for the employer to use an employee's personal information without that employee's consent requires an employer to establish that

1. the sole purpose for the collection, use or disclosure of employee personal information is to establish, manage or terminate the employment relationship,
2. the purpose for the collection, use or disclosure of employee personal information is itself reasonable, and
3. the collection, use or disclosure of employee personal information is reasonably required for that purpose.

In this case, the hotel established that it had until recently used signatures on paper for employee sign-in and -out. It had acquired an automated payroll system to produce more accurate payroll records. The system had a biometric capacity but, as an intermediate step, the hotel had used a swipe card alternative that proved unsatisfactory because of incompatibility with the hotel's door lock technology and problems with demagnetization. The finger scan was designed to verify the punch in and punch out of employees in place of using swipe cards for that purpose.

The hotel confirmed that the finger scan system was being used only for the purpose of verifying employees' identity as a match to the number they punch in, to ensure accurate payroll and accurate records of which employees are in the building in case of emergencies. The hotel had previously had instances of employees using the wrong number to punch in and out and a general concern of some employees punching in and out for one another. The hotel agreed to give its employees more comprehensive notice of its intention to implement a biometric scanner as part of its new payroll system and the complainant accepted our opinion that the hotel was authorized under PIPA to collect employee biometric information for payroll purposes.

### **... but Not in Others**

Another hotel that was upgrading its payroll system was also considering the implementation of a hand scanning system to record employees' payroll punch-in and punch-out transactions using biometrics technology. It introduced the system on a trial basis without notifying the union representing the hotel's employees. The union filed a grievance alleging that "the hotel has violated ... the *Personal Information Protection Act* by implementing a biometric hand scan system for time keeping which results in a search or physical examination of the employees' physical person and seizure of bodily information without consent. The union believes this practice violates the employees' right to privacy in their physical integrity."

In this case, the hotel had informed the union that its primary purpose for implementing the hand scan technology with its new payroll system was to use the most advanced available technology to position itself "to be a leader in service, quality and technology." The hotel acknowledged to us that it "does not have a bona fide need to use the hand scan system from an employee relations perspective" and stated that the purpose of the hand scan system was not for monitoring employees. Under the hotel's lease arrangements with the payroll system provider, it could exchange the hand scan system for a card swipe system.

We were of the view that the hotel had failed to establish that the employee personal information collected by the hand scanner was reasonably required for the sole purpose of managing the employment relationship. Its stated purpose for implementing the hand scan technology was to use the most advanced available technology to position itself as an industry leader in technology. We considered that purpose to be related to marketing the hotel, rather than to establishing or managing the employment relationship with its employees.

The hotel accepted our opinion that it was not authorized under PIPA to collect employee biometric information in these circumstances. The hotel notified the union representing its employees that it would not be implementing the biometric component of its new payroll system.

---

### **Job Applicant Objects to Collection of Excessive Information before Hiring**

A man who applied for a position with a national retail chain objected to being asked to provide his social insurance number (SIN) on the company's job application form. While we were investigating this complaint, we also looked at the form's requirement that applicants provide information on criminal history and identify any relatives that were already working for the company.

The company explained that many applications come from people who are not eligible to work in Canada and it collects the SIN as a way of screening them out. It argued that collecting information about an applicant's criminal history is a reasonable occupational qualification given that employees have access to cash and merchandise. Finally, the company justified the collection of names of spouses or other family members already employed on the basis that company policy prohibits employees from being in a reporting relationship with a family member.

Under the *Personal Information Protection Act*, businesses may only collect from job applicants information that is reasonably required to assess their suitability for a position. The SIN may only be collected after someone is hired because it is needed for income tax purposes. As a result of our investigation and mediation, the company agreed to change its job application form. In future, it will ask for only the first three digits of the SIN, thus providing the necessary information to the company without infringing on the applicant's right to keep that information confidential prior to hiring.

The company also agreed to restrict its requirement for information about criminal history by asking applicants to identify only whether they have been convicted of any of a list of particular criminal offences, such as theft or fraud, where that information is relevant to a fair assessment of their suitability for jobs with the company.

The company will ask applicants only to identify any position held by a relative. This will enable the company to manage compliance with its policies without identifying particular individuals on the application form.

### **Lock It or Lose It—Car Theft Nets Health Records Too**

People generally consider their medical records among the most sensitive type of personal information, and any inadvertent leak of personal health information causes public concern.

The driver for a health professional courier company, at one of his delivery locations in Langley, parked close to the doors of the building, collected the mail from the car, and entered the building, leaving the car running and unlocked. When he returned to the parking lot, the car, including all the mail that he had

picked up that day and all the undelivered mail, had been stolen. The mail included medical test results and correspondence concerning patient health information.

A few hours later, someone discovered part of the mail from the stolen car in a recycling bin. The car was later discovered in Edmonton. A second package of mail was recovered in front of a garbage disposal container near a retirement facility.

The courier company acted immediately to notify its clients, calling most of them the day of the theft and following up with a formal written notification to all clients. It also delivered the recovered mail to the appropriate recipient.

We initiated an investigation into whether the company had in place reasonable security arrangements to prevent unauthorized access or disclosure and had made every reasonable effort to prevent unauthorized access, as required by section 34 of the *Personal Information Protection Act*.

Our investigation concluded that the theft came about because the driver ignored explicit company information security policies of which he was aware. Despite the theft, the company had reasonable policies in place and made reasonable attempts to ensure that all employees were aware of and complied with those policies. The report also concluded that the company had taken all reasonable steps to contain the breach and retrieve the stolen records. Our office made recommendations to the company to enhance information security, which the company accepted.

### **Forged Consent Lands Mortgage Broker in Hot Water**

Organizations with access to databases of personal information must take care not to abuse the privilege. In this case, a mortgage broker, acting on the request of a client, agreed to submit a credit report request to Equifax, a company that maintains the credit histories and ratings of virtually all Canadians. The credit report was about a third party with whom the broker's client had had some business dealings. The third party did not know about the request nor did he consent to it.

All individuals in Canada are entitled to contact Equifax and request a copy of their credit report. Companies holding accounts with Equifax (such as banks, mortgage brokers, credit unions and retailers) request credit reports in order to determine whether to extend credit or enter into certain business transactions with individuals. However, the company must have the consent of the individual whose credit report is being requested. In this case, the authorization signature of the person whose credit report was being sought had been forged. The third party found out about this unauthorized action and complained both to our office

and to the Registrar of Mortgage Brokers at B.C.'s Financial Institutions Commission.

The OIPC began an investigation but deferred to the Registrar of Mortgage Brokers while the Registrar's staff conducted an investigation and a subsequent hearing that could have led to the imposition of penalties. Before the hearing, the mortgage broker admitted certain facts and entered into a consent order by which he was suspended for a period of time and agreed to pay the costs of the investigation.

The *Personal Information Protection Act* provides a process by which a complaint may be investigated and a mediated resolution attempted. If not settled during that process, the complaint may on request proceed to an inquiry at which the Commissioner or delegate may make a finding that a certain action was contrary to PIPA. Armed with the Commissioner's order, a complainant can then commence a court action for damages. In this case, the complainant was satisfied with the remedial measures imposed by the Registrar of Mortgage Brokers and chose not to pursue the PIPA matter any further.

### **Law Files Blowing in the Wind**

The confidentiality afforded a lawyer's client by way of the long-standing tradition of solicitor-client privilege means that law firms will routinely hold a great deal of personal information in their client files, be it matrimonial, tax, financial or medical information. For that reason law firms must be especially vigilant in ensuring that records are properly and securely destroyed when no longer required.

Certain law firms in Victoria and Vancouver will remember 2006 as the year they tightened up their document-handling practices. A law firm in Victoria was the subject of a complaint to the OIPC by a concerned citizen who spotted client records with the firm's letterhead beside a dumpster near the firm's offices, and a Vancouver firm made the evening news in an unhappy fashion when similar client records were found blowing in the wind outside the firm's office building.

What we found in investigating each instance was that firms were trusting cleaning staff or building maintenance personnel to take records intended for secure destruction and recycling to recycling bins, where they would later be picked up. At one firm, cleaning staff inadvertently mixed client records with regular garbage and put it in a nearby dumpster. In the other case, records intended for secure shredding, for reasons unknown, never made it to a locked bin that provided what was intended to be a secure recycling service to the building's commercial tenants.

In each case, the system for secure destruction of client records was inadequate. The OIPC recommended and monitored the introduction of privacy-protective practices at each firm, which included having locked recycling bins reserved

exclusively for sensitive records located in each firm's office rather than in a common building space or alleyway. These bins would then be emptied, and the client records securely shredded, by a contracted company specializing in secure document destruction. Cleaning staff or building maintenance personnel no longer play a role in the records management cycle. We considered the revised procedures adequate, but were left wondering how many other law firms might inadvertently be putting their clients at risk through inadequate document protection standards.

For that reason, we advised the Law Society of British Columbia (the governing body of the province's legal profession) about our concerns. The Law Society then sent a notice to its members reminding lawyers of the duty of client confidentiality set out in the *Professional Conduct Handbook* and of their privacy obligations under the *Personal Information Protection Act*. The notice provided a useful list of safeguards law firms should implement to protect client privacy.

## **6.2 Case Summaries: PIPA Requests for Review**

The following selected summaries illustrate the kinds of requests for review that the OIPC receives. Requests for review by the OIPC generally relate to a dispute about an individual's request to have access to her or his own personal information.

### **A Lawyer Paid Is a Law File Earned**

A client who has a parting of the ways with her lawyer and hires another should be able simply to pick up the file from the old office and deliver it to the new—unless she hasn't paid the bill. In that case, the unpaid lawyer might exercise what is called a "solicitor's lien" over the file materials, in which case the lawyer would hold the materials until the bill is paid.

A disaffected client who found his way to our office thought he had hit on a more imaginative way to get hold of his file: since the file materials contained his personal information and, since law offices are organizations subject to PIPA, the client requested a copy of his records under PIPA.

There was a slight problem: the information wasn't completely his. It was a matrimonial litigation file. The personal information of the client and his ex-spouse was so closely intertwined that to meet PIPA's requirements was next to impossible. PIPA makes it clear that a person may request his or her personal information from an organization, but not that of a "third party", meaning any other individual, such as the ex-spouse.

Some information-access matters just weren't meant to be solved by PIPA. Fortunately, PIPA itself provides a way out: section 38(4) provides that the

commissioner “may require an individual to attempt to resolve the individual’s dispute with an organization in the way directed by the commissioner before the commissioner begins or continues a review or investigation under this Act of an applicant’s complaint against the organization.”

The Commissioner directed that the client avail himself of the appropriate remedies provided by sections 77 and 78 of the *Legal Profession Act*. On this basis, the file was closed.

(After this case was resolved, PIPA was amended to permit lawyers to refuse to disclose to an individual her or his own personal information if it is in a document that is subject to a solicitor’s lien.)

### **Worker Seeks Records Proving Workplace Injury**

A woman involved in a worker’s compensation dispute with her former employer asked the company for certain information she felt would support her claim related to a carpal tunnel syndrome injury. She requested the name of the individual who had taken a photograph of her former workstation. She also asked for the names of former co-workers who had indicated to a manager that they remembered the applicant wearing a tensor bandage while at work.

The company responded by denying access to the identity of the photographer in accordance with section 23(4)(c) of PIPA. Moreover, it told her it had no record of the identities of the workers who had reported seeing the applicant wearing a tensor bandage at work.

PIPA gives applicants the right to request personal information only about themselves. It does not give them a right to request personal information about other individuals or general information about organizations. The name of the individual who took pictures of the applicant’s former workstation is not the applicant’s personal information. Therefore, PIPA did not require the company to disclose that information. The company confirmed that it had no record of the identities of the co-workers mentioned and no formal record of any statements that they may have made. The company, therefore, had no records responsive to this request and was in compliance with PIPA. The applicant accepted this assessment and agreed to close the file.

### **Insurance Company Asks Doctor to Vet Medical File Before Release**

A woman asked her private medical insurance provider for a copy of her medical file. To ensure that there would be no harm in disclosing the entire contents of the file to her, the company gave it to her doctor instead and told her she could access his copy. She complained to us that the company had improperly disclosed the copy of the file to her physician. She wanted the physician to return the file to the company and the company to provide a copy directly to her.

As a result of mediation by our office, the company gave the complainant a complete copy of her file. The disclosure to the physician was found to be in compliance with section 23(4)(b) of PIPA and of section 5(1) of the regulations to PIPA, which permits organizations to disclose information relating to the mental or physical health of the individual to a health care professional, for the purpose of obtaining an assessment from the health care professional as to whether the disclosure of that information could reasonably be expected to result in grave and immediate harm to the individual's safety or mental or physical health. The physician determined that there would be no harm in disclosure and persuaded the complainant to agree to his retaining a copy of her file, as he had incorporated it into her personal medical file.

### **6.3 Case Summaries: PIPA Orders**

Under PIPA, the commissioner has the ability to hold formal inquiries and issue orders that bind those involved. The following summarizes the formal orders issued to date under PIPA.

#### **Order P05-01—Collection of Personal Information by A Canadian Tire Store**

A woman returning goods to a Canadian Tire store was asked to provide her name, address and telephone number but declined to do so. Instead she complained to us about the inappropriate collection of information by the organization operating the store.

At the inquiry, the Commissioner found that the organization's notices of purpose of collection complied with PIPA, although he encouraged the organization to improve them. The Commissioner also found that PIPA permitted the organization to require individuals to provide this personal information and to use it as part of its efforts to detect and deter fraudulent returns of goods. He concluded that this information was "necessary" for that purpose under section 7(2) of PIPA.

The Commissioner also said, however, that the organization could not require individuals to provide such personal information for the purpose of customer satisfaction follow-up, a purpose and use that must be made optional for customers. Finally, he found that section 35(2) of PIPA did not authorize the organization to retain personal information permanently, but he did not suggest a retention period.

#### **Order P06-01—Access to Information in Dentist's Files**

The applicant requested access to her personal information in the hands of the organization, a dentist. The organization provided copies of the applicant's clinical records but refused access under sections 23(3)(a) and (c) and 23(4)(c)

and (d) of PIPA to its “College/Litigation file”, comprising 16 records related to the applicant’s complaint to the College of Dental Surgeons. The organization also said that it was not able to sever the records under section 23(5).

The Commissioner found that sections 23(4)(c) and (d) of PIPA did not apply to all of the information in the records and that severing under section 23(5) was possible. He also found, however, that the organization was authorized by section 23(3)(c) to refuse access to 15 records in their entirety and by section 23(3)(a) to refuse access to the sixteenth record.

### **Order P06-02—Access to information from two organizations**

The applicant requested his personal information in documents of two organizations, a law firm and the union whose members the firm had represented in a labour grievance. Both organizations were authorized and required to refuse disclosure under ss. 23(3) and (4), which respectively protect solicitor-client privilege and personal safety.

### **Order P06-03—An employee’s complaint to WorkSafeBC disclosed to fellow employees**

The complainant’s manager told other organization employees that the complainant had made a complaint of unsanitary workplace conditions to WorkSafeBC. This was not reasonable for the purposes of managing the employment relationship and was not otherwise authorized under PIPA. Since this was a one-off disclosure and the business’s ownership had changed, no remedy was ordered.

### **Order P06-04—Film Company Collects Employee Personal Information for Tax Credit Purposes**

Personal information collected by 20<sup>th</sup> Century Fox to establish an employee’s residency in British Columbia, in order to substantiate Fox’s claims for film production tax credits, were “employee personal information” and Fox’s collection, use and disclosure of it for that purpose complied with PIPA. PIPA requires an organization to provide information about its privacy policies on request, but it does not require the organization to provide a copy of its entire policy to whomever asks. Fox’s security arrangements for the employee personal information were reasonable.

### **Order P06-05—Work Product Information**

The organization, a travel agency, collected emails to and from three individuals that were sent and received using the organization’s email system. Much of the emails’ contents consisted of “work product information” and “contact information”, not personal information, but they also contained some personal

---

information of the complainants and other individuals. PIPA authorized the organization to collect, use and disclose that personal information for the purpose of its “investigation” into whether the complainants had breached their agreements with the organization.

**Order P06-06—Condo association has to give notice before collection, use and disclosure of employee personal information**

The organization was authorized to collect, use and disclose employee personal information without consent in most respects complained of here, but failed to give notice that it was doing so as required by PIPA. It also disclosed personal information contrary to PIPA in relation to some disclosures, failed to make reasonable security arrangements to protect personal information and failed to make a reasonable effort to assist the complainants as applicants. It did not fail to make a reasonable effort to ensure the completeness of personal information that it collected. Nor did it fail to retain personal information as required by PIPA. In view of the timing and nature of the organization’s failures to comply with PIPA, and the organization’s ongoing efforts to comply with PIPA, no legitimate purpose would be served by making any orders.

\* \* \*