Office of the Information & Privacy Commissioner for British Columbia

2007–2008 Annual Report

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

2007–2008 ANNUAL REPORT

Library and Archives Canada Cataloguing in Publication Data

British Columbia. Office of the Information and Privacy Commissioner.
Annual report
(CD-ROM)
Annual report [electronic resource]. –2005/2006–

Annual
CD-ROM format.
Issued also in printed form on demand.
Report year ends Mar. 31.
ISSN 1911-0278 = Annual report (British Columbia. Office of the Information & Privacy Commissioner. CD-ROM)

1. British Columbia. Office of the Information and Privacy Commissioner – Periodicals. 2. British Columbia. Freedom of Information and Protection of Privacy Act. 3. Privacy, Right of – British Columbia – Periodicals. 4. Government information – British Columbia – Periodicals. 5. Public records – British Columbia – Periodicals. I. British Columbia. Office of the Information and Privacy Commissioner. II. Title.

KEB505.62 342.711'062 C2006-960094-5
KF5753.I5B74

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

July 21, 2008

Bill Barisoff, MLA
Speaker
Legislative Assembly of British Columbia
Victoria, BC V8V 1X4

Dear Speaker:

According to s. 51 of the *Freedom of Information and Protection of Privacy Act* and s. 44 of the *Personal Information Protection Act*, I have the honour to present the Office's fourteenth Annual Report to the Legislative Assembly.

This report covers the period from April 1, 2007 to March 31, 2008.

Yours sincerely,

David Loukidelis
Information and Privacy Commissioner
for British Columbia

Mail: PO Box 9038, Stn Prov Govt, Victoria BC V8W 9A4
Location: 3rd Floor, 756 Fort Street, Victoria BC
T. 250 387 5629 F. 250 387 1696
Toll free through *Enquiry BC* 800 663 7867 or 604 660 2421 (Vancouver)
W. www.oipc.bc.ca

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER — for — British Columbia

TABLE OF CONTENTS

1 COMMISSIONER'S MESSAGE

1.1 Personal Information Goes Walkabout: Privacy Breaches on the Rise

In her most recent annual report, my federal colleague, Jennifer Stoddart, called last year the year of the privacy breach. There is no doubt that in British Columbia the number of breaches, which involve inappropriate access to personal information or the loss or theft of personal information from public bodies or private sector organizations, was up. We investigated 96 privacy breaches last year. The majority were caused by thefts of computers or vehicles that contained personal information in the form of computers or hard copy files. One public body alone had ten breaches, all involving the same program area and the same risk – workers taking records out of the office and leaving them in a car that was stolen or broken into. Another large category of breaches involves employee error or misconduct. Examples include a health care worker in a small town posting personal information from a hospital emergency ward on her blog and a secure-destruction company's employee stealing personal information on CDs.

Overall, the theme of the breaches last year was employee error. We have repeatedly reminded organizations and public bodies that ongoing employee training is a critical tool in preventing privacy breaches. Business organizations are starting to recognize the need for employee training and engagement. Organizations are now more aware of the need for their employees to be able to recognize a breach but also to avoid it. This will take on a new significance if PIPA is amended to implement the review committee's recommendation that individuals affected by a privacy breach be notified of the breach.

1.2 Where Are Your Information Security Holes?

Another important theme emerging from the past year is the apparent lack of awareness on the part of many public bodies and organizations of the weaknesses in their technical and administrative information security. This is bad for privacy. It is also bad news for the security of corporate or government information assets.

Both PIPA and FIPPA require public bodies and organizations to take reasonable measures to protect personal information. This is an evolving standard in terms of technical protections and process safeguards. It is abundantly clear to me, however, that organizations and public bodies alike should be taking an inventory of their personal

information holdings. They should also be regularly assessing their security arrangements for personal information holdings, and identified weaknesses must be fixed promptly. This is almost certainly much cheaper than fixing risks after a privacy breach has occurred. The OIPC has repeatedly recommended both regularly scheduled and spot internal audits and reviews to ensure compliance with security standards under PIPA and FIPPA. We are also working on a diagnostic information security checklist for both the private and public sectors.

1.3 Privacy and Electronic Health Records

During the last session of the Legislative Assembly, the government introduced Bill 24, the *E-health (Personal Health Information Access and Protection of Privacy) Act*, in order to govern e-health information systems, including the one the Ministry of Health Services is now developing. That system will, essentially, be a network of integrated information and communication technologies that allows a range of authorized users immediate and up-to-date access to patient information. The electronic health records system will, it is said, offer significant benefits to patients in the form of improved outcomes, reduction in adverse drug interactions and improved access to health care. It is also said to improve health planning and program delivery.

At the same time, the Supreme Court of Canada has confirmed that personal health information has special protection, as Canadians rightly expect. The benefits of EHR systems aside, it is clear they can raise significant challenges for privacy in three key areas. The first relates to access controls. Key policy choices must be made in deciding which of many thousands of health system workers will have access to patient information. Second, meaningful audit controls have to be built into such systems to catch those who wrongly browse through or use patient information.

Last, but by no means least, it is imperative that patients have a meaningful degree of control over disclosure and use of their personal health information. This fundamental principle is at the core of internationally recognized privacy norms and it must be a feature of British Columbia's EHR systems. A key aspect of patient choice is access by patients to their own personal health information. This is another internationally affirmed privacy principle.

Bill 24 supports both of these principles, on paper, by requiring the government to give individuals meaningful control over disclosure and use of their personal health information and to give patients access to their own information. I will adamantly oppose any attempt to water down patient control and access by building a system that does not deliver on these legislated commitments to the public. In the coming year, we will actively monitor development of the provincial EHR system and vigorously push for meaningful patient control and access in practice, not just in the statute books.

1.4 Ongoing Delays in Responding to Access Requests

A number of my annual report messages have targeted public body delays in responding to access to information requests. This is now clearly a chronic problem at the provincial government level – a problem that predates my becoming commissioner in 1999 and continues to be of grave concern. It is often said that access delayed is access denied, and the inability of the citizens to exercise their rights to information under FIPPA in a timely way is cause for grave concern.

The ongoing failure by provincial government ministries to respond overall to requests in a timely fashion is particularly troubling because FIPPA's time limits were materially relaxed in 2003 by changing the response time to 30 business days instead of 30 calendar days. Despite this generous change, responses by provincial government ministries to requests for general information – as opposed to requests for personal information – took an average of 51 business days, not calendar days, in fiscal years 2006-2007and 2007-2008. The average response time for personal information requests in 2007-2008 was 26 business days, which, combined with the general information response average, yielded an overall average of 35 business days. Even this combined average is outside the relaxed 30 business day response time introduced in 2003.

In 2006, my concern that public bodies were not responding when FIPPA requires it led me to create a new fast-track process for dealing with such 'deemed refusals' of access. The goal was to ensure that public bodies seek extension of FIPPA's response timelines, as they are supposed to do. This has drastically reduced the number of deemed refusals. Not surprisingly, however, the OIPC has seen significant increases in requests for extensions of the time to respond. These went from 242 to 352 at the end of fiscal year 2007-2008. In more than 50% of those requests, the ministry seeking more time cited lack of resources for processing requests or retrieving records, or both, as factors contributing to the delay and thus the need for extension.

This illustrates a serious and ongoing problem with delay. In the end, this is about money, plain and simple. Access and privacy staff are dedicated, hard-working professionals, but they can only do so much. More is needed, and that means more money for more staff. For this reason, last December we met with assistant deputy ministers responsible for corporate services in the various ministries. We urged them to ensure that increased resources are dedicated to access and privacy functions in their ministries. I will again be meeting with them to do everything possible to ensure that, beginning in fiscal 2008-2009, ministries dedicate sufficient resources to comply with their legal obligations for openness and accountability to the people of British Columbia.

I have decided that other steps are necessary to bring pressure to bear on this untenable situation. Beginning later in 2008, the OIPC will begin a program of compliance report cards for ministries. Each ministry will be rated at least annually according to published performance criteria, which will include compliance standards for timeli-

ness in their access responses. Each performance report will be directed to the head of the ministry, will be published on the OIPC website and will otherwise be publicized. My goal is to alert ministries and stakeholders to compliance problems so they can be remedied promptly. Another goal, of course, is to report where a ministry is doing well and to acknowledge that success. The office of my federal colleague, the Information Commissioner of Canada, has had a similar system of compliance reporting for several years. At the time of writing, that office is in the process of revamping its assessment and reporting system and has generously agreed to support development of our own system in the coming months.

It is important to underscore here that, consistent with the OIPC's long-standing approach, we will work as constructively as possible with the affected ministries, and with affected requesters, to address these problems meaningfully. In doing so, we recognize that, as critical as proper funding might be, other factors contribute to success in meeting FIPPA's requirements. The following factors, among others, will influence the performance criteria that we develop for our compliance reports:

- the nature and degree of meaningful senior executive support for the access and privacy branch and functions within the ministry;
- whether there are sufficient numbers of employees with necessary expertise in access and privacy;
- whether there are sufficient numbers of records management staff in the operational parts of the ministry who are capable of searching, and can search, in a timely fashion for both paper and electronic records;
- whether the ministry uses a central filing system for records (it takes public bodies significantly longer to find records, and sometimes records are missed, if public bodies allow individuals to create their own copies of files or to file records inside individual offices or on desktop computer drives); and
- whether the ministry has an efficient and fair sign-off process (e.g., a process with limited sign-off requirements and delegation of decision-making authority to the appropriate experts).

My emphasis is on finding collaborative and mutually beneficial solutions to these pressing problems with compliance. I will be following up with each Assistant Deputy Minister of corporate services in each ministry to determine what steps they have taken, including increases in budget resources for access and privacy branch functions and records retrieval functions, to address compliance with their ministries' statutory duties. Positive steps will be publicly acknowledged for the leadership shown. In other cases, the OIPC will review the situation and determine what investigative steps, or public reporting measures, are appropriate to find other solutions to these pressing and serious problems.

1.5 Developments on the Legislative Front

In last year's message, I said that our experience with the *Personal Information Protection Act* ("PIPA") over the last number of years has been that it is working well. The all-party committee of the Legislative Assembly that was reviewing PIPA at the time has since made a number of recommendations for amendments to PIPA. It is safe to say that the committee's report confirms that PIPA is, in fact, working well on the whole. The committee's thoughtful analysis and sound recommendations for amendments will improve PIPA on a number of fronts, while respecting the balanced and effective legislative framework and policy choices reflected in that law. The committee's recommendations are also consistent with recommendations made in the legislative reviews of the federal *Personal Information Protection and Electronic Documents Act* and Alberta's *Personal Information Protection Act*. I congratulate the committee on its well-received report and urge the government to move forward with legislative amendments implementing the committee's recommendations at the earliest opportunity.

Another theme of my last message was that yet another year had slipped away since unanimous Legislative Assembly Review committee recommendations were made, in 2004, to improve the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). When I wrote this time last year, a Bill had been tabled with a number of important amendments that flowed from the committee's work, but the Bill did not proceed. I am happy to report that, during this last legislative session, the same amendments proceeded and basic improvements to FIPPA have been made.

While these amendments are important, and very welcome, they do not include an absolutely critical piece, which the review committee had unanimously approved on an all-party basis. Section 13 of FIPPA, which is intended to protect advice or recommendations developed by or for public bodies, still urgently needs to be fixed. This is crucially important if we are to restore the intended scope and meaning of that provision. As I said last year, the Premier and Cabinet have an excellent opportunity to show strong leadership in openness and accountability by amending section 13 of FIPPA in line with the 2004 all-party committee recommendations. As the government increasingly defines its role as steering rather than rowing the ship of government, decisions around what course to take is a matter of great public importance. I call on them again to reinstate the access rights the citizens of British Columbia have lost.

1.6 Moving Forward

This past year brought us a variety of new challenges, while some older ones – including the struggle to make ends meet – continued to confront us. We are in the process of finalizing reforms to our investigation and dispute resolution processes and are looking, as always, for new ways to do our work. As we move into the new fiscal year, we remain dedicated to protecting privacy and the right of access to information.

David Loukidelis
Information and Privacy Commissioner for British Columbia
July 2008

2 THE YEAR IN REVIEW: STATISTICAL HIGHLIGHTS

The following tables provide a detailed summary of our activities with respect to both the *Freedom of Information and Protection and Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). Explanatory notes following each table clarify terms used in the table and the significance of various totals.

TABLE 1. FIPPA AND PIPA FILES RECEIVED AND CLOSED, 1 APRIL 2007 – 31 MARCH 2008

	DISPOSITION			
FILE TYPE	RECEIVED 07/08	CLOSED 07/08	RECEIVED 06/07	CLOSED 06/07
Information requested/received				
Requests for information	2832	2832	2783	2781
Read and file	90	88	99	98
Media queries	45	31	39	37
Freedom of information requests for OIPC records	8	5	4	4
Requests for review				
Requests for review of decisions to withhold information	695	578	598	655
Applications to disregard requests as frivolous or vexatious	8	8	6	5
Complaints				
Complaints about non-compliance with FIPPA or PIPA	449	452	455	454
Reviews/investigations declined				
Non-jurisdictional	30	30	29	27
No reviewable issue	99	91	104	103
Requests for time extension				
By public bodies/organizations for time extension	352	352	242	244
By applicants for time extension to request a review	11	12	17	18
Reconsideration of decisions				
Internal reconsideration of OIPC decisions	33	30	5	4
Adjudication	4	0	1	1
Files initiated by public bodies/organizations				
Privacy impact assessments	4	1	9	9
Public interest notification	7	6	7	7
Notification of privacy breaches	92	97	86	72
OIPC-initiated files				
Systemic investigations	11	11	10	10
Special projects	21	18	28	20
Reviews of proposed legislation	43	39	52	55

TABLE 1. *continued*

	DISPOSITION			
FILE TYPE	RECEIVED 07/08	CLOSED 07/08	RECEIVED 06/07	CLOSED 06/07
Policy or issue consultations	108	76	133	112
Public education/outreach				
Speaking engagements by OIPC staff	58	55	57	50
Conference attendance	18	21	13	10
Meetings with public bodies/organizations	30	25	34	30
Site visits by Commissioner to public bodies/organizations	1	1	3	3
Other	9	8	14	16
Totals	**5058**	**4859**	**4828**	**4825**

TABLE 1 EXPLANATORY NOTES:

Information requested/received. Members of the public and organizations contact us regularly with questions about FIPPA and PIPA requirements. "Read and file" refers primarily to correspondence copied to the OIPC.

Requests for review. Our largest activity each year involves processing requests for review of decisions by public bodies and organizations to withhold information. The 578 requests for review we completed this year included 522 under FIPPA (Table 2) and 56 under PIPA (Table 8). On rare occasions, public bodies apply to have such requests dismissed as frivolous or vexatious under section 43 of FIPPA and section 37 of PIPA authorizes private organizations to make similar applications.

Complaints. The 452 complaint files closed this year included 331 under FIPPA, of which 247 related to access to information and 84 related to protection of privacy (Tables 4 and 5). The 121 PIPA complaints (Table 7) represented a one-third increase from the previous year.

Reviews/investigations declined. We may decline to investigate a complaint for a number of reasons (e.g., the complaint is frivolous or vexatious, no remedy is available or we do not have jurisdiction to examine the matter). When we decline to investigate a complaint or conduct a review because we lack jurisdiction, we try to direct the complainant or applicant to the appropriate body with the authority to address the concern (e.g., the federal Privacy Commissioner for private sector complaints against organizations that are not provincially regulated or the RCMP for complaints against that organization). In addition, we receive complaints against bodies such as BC Ferries that government has specifically excluded from the application of FIPPA.

Requests for time extension. Section 10 of FIPPA and section 31 of PIPA authorize public bodies and organizations respectively to ask our office for a time extension to respond to an access request under certain circumstances. Section 53 of FIPPA and section 47 of PIPA authorize applicants to ask us for permission to request a review more than 30 days after notification of the public body's or organization's decision. The Commissioner's Message at the beginning of this report comments on the significant increase this year in requests by public bodies for time extensions in responding to access requests.

Reconsideration of decisions. If a complainant presents new information after we have completed an investigation, we may reconsider our findings in light of that information. "Adjudication" in this instance refers to a review by a judge of a complaint about a decision, act or failure to act by the Commissioner as head of a public body.

Files initiated by public bodies or organizations. Public bodies and private organizations frequently ask us for advice on privacy/access implications of proposed policies or current issues or may ask us to review privacy impact assessments they have prepared for proposed policies or programs. Section 25 of FIPPA requires public bodies to disclose certain information in the public interest and to first notify us.

OIPC-initiated files. Investigations of individual complaints may trigger concerns about systemic issues in the operations of a public body, leading to broader investigations. Special projects include initiatives such as policy research and preparation of guidelines for FIPPA and PIPA compliance published on our website. In addition to reviewing all bills presented to the Legislative Assembly for FIPPA or PIPA implications, we provide advice on the drafting of bills at the invitation of public bodies.

Public education and outreach. Our public education activities include frequent presentations to community groups, business organizations and conferences on current issues, as well as information on complying with PIPA and FIPPA. We also meet individually with public bodies and organizations as the need arises and the Commissioner conducts site visits to assess and provide advice on compliance with the laws we administer.

TABLE 2. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY TYPE

	DISPOSITION								
TYPE	CONSENT ORDER	MEDIATED	NO REVIEWABLE ISSUE	NON JURISDICTIONAL	REFERRED TO PUBLIC BODY	WITHDRAWN	OTHER DECISION BY COMMISSIONER	NOTICE OF INQUIRY ISSUED	TOTAL
Deemed refusal	6	70	13	0	3	14	5	1	**112**
Deny access		48	3	2	0	13	1	12	**79**
Notwithstanding (s. 79)		2	0	1	0	2	0	0	**5**
Partial access		240	1	2	1	40	2	16	**302**
Refusal to confirm or deny		1	0	0	0	0	0	0	**1**
Scope		7	1	0	0	0	0	1	**9**
Third party		5	1	0	0	3	1	4	**14**
Total	**6**	**373**	**19**	**5**	**4**	**72**	**9**	**34**	**522**

TABLE 2 DEFINITIONS:

Consent order: OIPC order, following deemed refusal and with agreement of parties, specifying final date for public body response
Deemed refusal: Failure to respond within required timelines (s. 7)
Deny access: All information withheld from applicant (ss. 12-22)
Notwithstanding: Conflict between FIPPA and other legislation (s. 79)
Partial access: Some information withheld from applicant (ss. 12-22)
Refusal to confirm or deny: Refusal by public body to confirm or deny the existence of responsive records (s. 8)
Scope: Requested records not covered by FIPPA (ss. 3-4)

TABLE 3. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY PUBLIC BODY

	DISPOSITION								
PUBLIC BODY TOP 10 (top 10, by number of requests)	CONSENT ORDER	MEDIATED	NO REVIEWABLE ISSUE	NON JURISDICTIONAL	REFERRED BACK TO PUBLIC BODY	WITHDRAWN	OTHER DECISION BY COMMISSIONER	NOTICE OF INQUIRY	TOTAL
Insurance Corporation of BC	0	108	2	0	1	6	0	5	**122**
Vancouver Police Department	0	21	1	0	0	2	1	3	**28**
Ministry of Public Safety and Solicitor General	0	9	3	0	0	4	0	4	**20**
Ministry of Attorney General	0	9	2	0	0	3	0	1	**15**
Ministry of Health	0	11	0	0	0	2	0	2	**15**
BC Lottery Corporation	2	5	0	0	0	3	0	5	**15**
Ministry of Children and Family Development	0	10	0	1	1	2	0	0	**14**
Vancouver Coastal Health Authority	2	8	0	0	0	4	0	0	**14**
Ministry of Forest and Range	0	9	0	0	0	2	0	0	**11**
Vancouver Island Health Authority	0	9	0	0	0	1	0	0	**10**
Top 10 totals	4	199	8	1	2	29	1	20	**264**
All other public bodies	2	174	11	4	2	43	8	14	**258**
Total	**6**	**373**	**19**	**5**	**4**	**72**	**9**	**34**	**522**

TABLE 3 EXPLANATORY NOTES:

The great majority of ICBC requests for review are filed by lawyers performing due diligence on behalf of clients involved in motor vehicle accident lawsuits. As with ICBC, the number of requests for review and complaints against a public body is not necessarily indicative of non-compliance but may be a reflection of its business model or of the quantity of personal information involved in its activities.

TABLE 4. DISPOSITION OF FIPPA ACCESS COMPLAINTS, BY TYPE

	DISPOSITION										
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED BACK TO PUBLIC BODY	NO REVIEWABLE ISSUE	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	REPORT ISSUED	TOTAL
Adequate search	16	15	3	1	17	1	4	1	0	0	**58**
Duty required by Act	23	16	6	14	32	11	12	4	1	1	**120**
Fees	22	4	3	1	12	0	7	0	4	0	**53**
Time extension by public body	2	5	1	3	2	3	0	0	0	0	**16**
Total	**63**	**40**	**13**	**19**	**63**	**15**	**23**	**5**	**5**	**1**	**247**

TABLE 4 DEFINITIONS:

Adequate search: Failure to conduct adequate search for records (s. 6).
Duty required by Act: Failure to fulfil any duty required by FIPPA (other than an adequate search).
Fees: Unauthorized or excessive fees assessed by public body (s. 75).
Time extension: Unauthorized time extension taken by public body (s. 10).

TABLE 5. DISPOSITION OF FIPPA PRIVACY COMPLAINTS, BY TYPE

	DISPOSITION										
TYPE	MEDIATED	SUBSTANTIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	REFERRED BACK TO PUBLIC BODY	NO REVIEWABLE ISSUE	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	REPORT ISSUED	TOTAL
Collection	1	3	1	0	4	3	0	0	0	0	**12**
Correction	5	1	0	1	10	1	1	0	0	0	**19**
Disclosure	3	15	5	7	7	6	2	3	0	1	**49**
Retention	0	0	0	0	0	0	0	0	0	0	**0**
Use	0	1	0	0	0	2	0	0	0	0	**3**
Notification	0	1	0	0	0	0	0	0	0	0	**1**
Total	**9**	**21**	**6**	**8**	**21**	**12**	**3**	**3**	**0**	**1**	**84**

TABLE 5 DEFINITIONS:

Collection: Unauthorized collection of information (ss. 26 and 27).
Correction: Refusal to correct or annotate information in a record (s. 29).
Disclosure: Unauthorized disclosure by the public body (s. 33).
Retention: Failure to retain information for time required (s. 31).
Use: Unauthorized use by the public body (s. 32).
Notification: Disclosure of information in the public interest (s. 25).

TABLE 6. DISPOSITION OF FIPPA ACCESS AND PRIVACY COMPLAINTS, BY PUBLIC BODY

	DISPOSITION									
PUBLIC BODY (Top 10, by no of complaints)	ADEQUATE SEARCH	COLLECTION	CORRECTION	DISCLOSURE	OTHER DUTY REQUIRED BY ACT	FEES	RETENTION	TIME EXTENSION BY PUBLIC BODY	USE	TOTAL
Ministry of Public Safety and Solicitor General	9	0	1	2	8	2	0	0	0	**22**
Insurance Corporation of BC	2	2	1	5	6	0	0	1	0	**17**
Ministry of Attorney General	6	0	1	1	7	0	0	2	0	**17**
Ministry of Children and Family Development	3	4	2	4	3	0	0	0	1	**17**
Vancouver Coastal Health Authority	1	0	2	3	7	1	0	0	0	**14**
Vancouver Police Department	3	0	4	1	5	1	0	0	0	**14**
Ministry of Health	1	1	0	0	9	3	0	0	0	**14**
WorkSafeBC	4	1	0	3	3	1	0	0	0	**12**
Ministry of Forest and Range	3	1	0	0	2	2	0	1	0	**9**
Ministry of Environment	1	0	0	1	3	2	1	0	0	**8**
Top 10 totals	33	9	11	20	53	12	1	4	1	**144**
All other public bodies	25	3	8	29	67	41	0	12	2	**187**
Total	**58**	**12**	**19**	**49**	**120**	**53**	**1**	**16**	**3**	**331**

TABLE 7. DISPOSITION OF PIPA COMPLAINTS, BY TYPE

	DISPOSITION									
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED BACK TO ORGANIZATION	NO REVIEWABLE ISSUE	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	TOTAL
Adequate search	2	3	1	2	3	0	2	1	0	**14**
Collection	3	7	4	1	11	1	7	2	1	**37**
Correction	5	1	0	0	2	1	0	0	0	**9**
Disclosure	4	6	2	1	8	2	0	1	0	**24**
Duty required by Act	5	3	0	2	3	4	1	0	1	**19**
Fees	3	1	0	0	1	0	1	0	2	**8**
Protection/retaliation	1	1	1	1	0	0	0	0	0	**4**
Retention	1	0	0	0	0	0	1	0	0	**2**
Use	0	1	1	0	1	1	0	0	0	**4**
Total	**24**	**23**	**9**	**7**	**29**	**9**	**12**	**4**	**4**	**121**

TABLE 7 DEFINITIONS:

Adequate search: Failure to conduct adequate search for records (s. 28).
Collection: Inappropriate collection of information (s. 11).
Correction: Refusal to correct or annotate information in a record (s. 24).
Disclosure: Inappropriate disclosure of personal information (s. 17).
Duty required by Act: Failure to fulfil any duty required by PIPA (other than an adequate search).
Fees: Unauthorized or excessive fees assessed by organization (s. 32).
Protection/retaliation: Reprisal against employee (s. 54).
Retention: Failure to retain personal information for time required (s. 35).
Use: Inappropriate use of personal information (s. 14).

TABLE 8. DISPOSITION OF PIPA REQUESTS FOR REVIEW, BY TYPE

	DISPOSITION							
TYPE	MEDIATED	NO REVIEWABLE ISSUE	NON JURISDICTIONAL	REFERRED BACK TO ORGANIZATION	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	TOTAL
Deemed refusal	32	2	0	0	6	0	0	40
Deny access	6	2	0	2	2	0	1	13
Partial access	3	0	0	0	0	0	0	3
Total	**41**	**4**	**0**	**2**	**8**	**0**	**1**	**56**

TABLE 8 DEFINITIONS:

Deemed refusal: Failure of organization to respond to request for personal information (s. 28).

Deny access: All personal information withheld from applicant (s. 23).

Partial access: Some personal information withheld from applicant (s. 23).

3 CASE SUMMARIES: FIPPA MEDIATIONS AND ORDERS

When we receive either a complaint alleging that a public body has breached FIPPA or a request for a review of a decision by a public body in response to an access to information begin request, we first determine that the matter is within our jurisdiction. We then analyze the application of FIPPA to the issues raised with us and begin communicating with both the applicant / complainant and the public body to see whether we can facilitate an informal resolution that is satisfactory to both parties.

The most common cause of disputes, in the information and privacy world as in any other dealings between ordinary citizens and organizations, is communication breakdowns that have little to do with legal rights or obligations. Simply by engaging in respectful and focused discussion with both parties to a dispute and exploring options for resolution, we are often able to bring about outcomes that both sides can live with and that comply with the law.

Applicants or complainants who don't get an initially hoped for result may still feel that our involvement has produced a benefit if we can explain the justification for public body decisions or actions that hadn't previously been understood. Conversely, if we believe a public body appears to have breached FIPPA or, in making a discretionary decision, has failed to consider and apply appropriate criteria, we will make our views known and, where applicable, explain why a Commissioner's order would be likely to go against the public body. Finally, mediation frequently produces alternative solutions that may differ from the result initially sought but prove just as satisfactory once identified and achieved.

We follow parallel procedures in handling complaints and requests for review under PIPA. On the infrequent occasions when applicants or complainants are unhappy with the results of mediation and continue to believe that their legal rights under FIPPA or PIPA have been unfairly breached, they may ask that the matter proceed to a hearing by the Commissioner or one of our adjudicators. A selection of order summaries follows the mediation summaries below, which are grouped by the statutory sections to which they relate.

3.1 FIPPA Mediation Summaries

SECTION 3: SCOPE OF THE ACT

1 Releasing Test Answers Would Reveal Test Questions

A woman attending a Lower Mainland university asked for a copy of her final exam. The university replied that it was unable to grant access because the exam was outside the scope of FIPPA, being "a record of a question that is to be used on an examination or test" under section 3(1)(d).

The purpose of section 3(1)(d) is clear – it protects information that, if disclosed, might give an applicant an unfair advantage in a competition by seeing the examination questions in advance of the examination, thus rendering a prepared examination ineffective for future use. The final exam in this case contained two parts: the questions and an answer booklet containing the woman's answers to the questions. The university withheld both. The university had used the exam questions in the past and intended to use them again in the future. As such, section 3(1)(d) clearly applied to the exam questions.

Could the university also use the same section to withhold the answers? It took the position that it should do so where a person's answers could be used to re-create the questions. Given the underlying intent of section 3(1)(d), we considered this to be a reasonable interpretation. Further, in reviewing the questions and answers in this case, we agreed that the answers could be used to re-create the questions and, therefore, that section 3(1)(d) also applied to the exam answers.

2 In Whose Custody Is a Diary on a Work Computer?

A public body employee complained that someone in the office had improperly accessed records on his work computer, including a diary and a private letter. The public body was unable to confirm or deny whether the employee's computer had been improperly accessed because it did not have an audit trail on the computer at the time of the alleged incident.

The first step in deciding the course of our investigation was to determine whether the records in question were in the custody or under the control of the public body, thereby placing them within the scope of FIPPA under section 3(1).

The courts have examined which factors indicate "custody" or "control" of records by a public body. For example, in the Matter of the Decision of the Information and Privacy Commissioner of British Columbia (Order No. 308-1999), 2000 BCSC 929, in paragraph 25, the Honourable Justice Shabbits agreed with the following comments by the Commissioner:

(a) that custody of records requires more than that the records be located on particular premises;

(b) that in order for a public body to have custody of records, the public body must have immediate charge and control of the records, including some legal responsibility for their safe keeping, care, protection or preservation; and
(c) that "custody" in FIPPA reflects a choice by the Legislature to limit FIPPA's application to "government" records, and not to personal records of employees that happen to be located on public body premises.

We found that the record was not created by a staff member in the course of his or her duties and that the contents of the records were neither used by the organization nor a record that related to the public body's mandate and functions. The public body had no authority to regulate the record's use and disposition and had not relied upon the record in any way.

As the records in question were not in the custody or control of the public body, we had no jurisdiction to proceed further and therefore terminated our investigation of the complaint.

SECTION 6: DUTY TO ASSIST APPLICANTS

3 Student Seeks Information on Campus Security Helpers

A student attending night classes made frequent use of a "safe walk" program that provided a campus security escort to the parking lot or bus stop. Campus security staff also helped her when some of her belongings were stolen. Four years later, the student asked the college to give her copies of the records documenting the assistance provided to her.

The college later responded that campus security had searched for the records the student had requested but had found none. She was told that at the time of her dealings with campus security there had been no consistent procedure for creating such records.

The student complained to us that the college had not conducted an adequate search, as she recalled some of the security officers making notes in her presence. The college provided a more detailed explanation that campus security had searched for records in their 2002 files, their current data base and a collection of slips of paper relating to safe walks. They had also contacted some retired security officers who recalled having assisted the student but had not retained any records themselves.

Section 6(1) of FIPPA requires public bodies, including universities and colleges, to make every reasonable effort to assist applicants. This creates an obligation to conduct an adequate search for requested records. Our office's decisions confirm that, to be considered adequate, a search must be thorough and comprehensive and that a public body must make a reasonable effort to explore all avenues. It is not a standard of perfection but requires diligence.

We concluded that, under the circumstances, the college had conducted an adequate search and, moreover, had no obligation to keep records of the nature sought for such a lengthy period of time. However, we did recommend that campus security implement a records management policy including provision for retention and destruction.

4 Law Graduate Stymied in Request for Year and Class Rankings

A recent law school graduate requested two pieces of information from the university where he had obtained his degree:

1) his overall rank in each of the three years of study; and

2) his ranking in each of the classes he took in each of the years.

The university responded by providing an overall ranking list for one of the applicant's years of study, with the names of the other students removed. It said that as the Faculty of Law had abolished compiling and issuing an overall ranking of its students the following year and had never ranked the students on a class-by-class basis, this information was not available.

The graduate complained to us that the university had failed to meet its duty under section 6 of FIPPA to "make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely". He believed that the information he had requested on overall ranking must be available as it was used in the awarding of prizes and scholarships. Further, he argued that if the university did not have that information at hand, section 6(2) required it to create the records for him. Section 6(2) reads:

> 6(2) Moreover, the head of a public body must create a record for an applicant if
>
> (a) the record can be created from a machine readable record in the custody or under the control of the public body using its normal computer hardware and software and technical expertise, and
>
> (b) creating the record would not unreasonably interfere with the operations of the public body.

The university explained to us that creating the records the complainant had requested would necessitate hiring a programmer to write a program, test the program and then produce the records. It interpreted FIPPA as not imposing an obligation to incur the significant effort and expense required in this case to create a record that did not already exist.

In submitting his complaint to us, the graduate suggested an alternative remedy. If the university was not obliged to create the records he was seeking, he asked to receive instead copies of the class grades for each of the courses which he took (with the other students' names redacted) so that he could count the number of students who received higher grades than he did. We confirmed with the university that this information could be produced from its existing systems and that it was willing to create these records if doing so would resolve the complaint. The graduate agreed to this resolution.

We always encourage requesters and public bodies to work together to devise alternative solutions to produce the required information if it is not available in the format initially requested, and in this case it was helpful that the complainant had considered alternatives before seeking our assistance.

5 Dangerous Offender Research Meets Privacy Invasion Obstacle

A researcher asked the Forensic Psychiatric Services Commission for information related to the assessments of dangerous offenders, including a list of the experts who performed the assessments, a list identifying which expert did which offender's assessment, and copies of the contracts and invoices related to each assessment over the last few years. The researcher suggested that if the names of the dangerous offenders could not be released, they be identified by their initials.

The Commission transferred the request to the Provincial Health Services Authority, which had control of the records. The PHSA released records to the applicant but refused to disclose the names or initials of the dangerous offenders to whom the records related. As its authority to deny access, the PHSA cited section 22(1) of FIPPA, a mandatory exception to disclosure that requires a public body to refuse to disclose personal information if disclosure would cause an unreasonable invasion of privacy to the individual the information is about.

The researcher then asked the PHSA to release the dangerous offender hearing number or create a unique identifying number for each dangerous offender so that he could differentiate between offenders referenced in the records. The PHSA refused to disclose the dangerous offender hearing number, again citing section 22, adding that FIPPA did not oblige it to create a record in which the dangerous offenders could be differentiated.

The researcher then asked us to review the PHSA's decision to deny access to the offenders' identifying information. One of the records released by the PHSA was a computer-generated spreadsheet listing each assessment for the time period requested. The spreadsheet included the date of the assessment, the name of the dangerous offender receiving the assessment, whether the assessment was an original assessment or a re-assessment, and the name of the expert who did the assessment. The information that identified each offender was severed from the record.

During mediation we suggested the spreadsheet could be manipulated to separate and group each offender on the spreadsheet. This way the researcher could see when and by whom an offender had been assessed and whether there had been any further assessments of the same offender. We concluded that section 6(2) of FIPPA required the PHSA to modify the spreadsheet in this manner insofar as it requires a public body to create a record if it can be done using the public body's normal computer hardware, software and technical expertise without interfering with the operations of the public body.

The researcher agreed to this resolution as it would provide him with the information he wanted. The PHSA also agreed on the condition that the researcher withdraw other complaints he had filed with our office related to the same request. We do not have the authority to ask an applicant to withdraw his appeals as a condition of resolving a complaint, and we would never deny an applicant the right to a review or an inquiry because of any agreement made with a public body. Consequently, we informed the PHSA that any agreement it reached with the applicant would not preclude him from asking to have the matter settled by inquiry.

In any event, the PHSA and the applicant managed to negotiate an agreement on how to resolve the matter. The PHSA, however, requested another condition – that the applicant sign a release permitting the PHSA to disclose the agreement to the Commissioner if the matter went to inquiry. Normally, negotiations that take place during mediation are not disclosed to the Commissioner during his consideration of the facts at an inquiry. We again had to tell the PHSA that we could not support this condition and it would again be up to the applicant and the PHSA to make an independent agreement. At this point, the researcher was frustrated with the delays and refused to sign a release.

Instead, the researcher requested that the matter proceed to an inquiry. Mediation continued as preparations were made for the inquiry, and the PHSA revised its proposal to modify the spreadsheet and agreed to provide the spreadsheet if the applicant agreed to drop his appeals, without conditions, with our office. The applicant agreed, received the spreadsheet and abandoned the inquiry.

SECTION 7: TIME LIMIT FOR RESPONDING; AND SECTION 8: CONTENTS OF RESPONSE

6 City Responds in Time, but Reasoning for Refusing Access Shaky

A man who emailed an access to information request to a city for internal correspondence complained that the city had not responded to his request in time, had not provided a reason for withholding one record and had not informed him of his right to ask us to review the city's response.

Section 7 of FIPPA requires a public body to respond to an access request within 30 business days. The complainant had not understood that "day" meant business day – the city had responded in time.

Section 8(1)(c)(i) requires a public body that refuses disclosure to give reasons for the refusal and the provision of FIPPA on which the refusal is based. In this case, the city had told the requester that it was withholding the record under section 12(1). When we pointed out that section 12(1) applies to Cabinet confidences at the provincial level, not local governments, the city realized its mistake and explained that it had intended to cite section 13(1), which applies to advice to a public body. As access to the record remained the complainant's ultimate objective, we opened a separate request-for-review file to address that matter and consider the city's section 13(1) argument.

The third part of the complaint related to the obligation of the city, under section 8(1)(c)(iii), to inform the requester of his right to request a review by our office of the city's decision to withhold information. The fact that his access request to the city had been by email and perceived to be of an informal nature made no difference to its validity, as the *Electronic Transactions Act* provides that a requirement for a document to be "in writing" includes electronic means; in addition, he had emphasized that "you can consider this a written request via Freedom of Information and Privacy Act". He was thus correct that the city had had an obligation to advise him of his FIPPA right to ask us to review the city's decision, and we therefore found this part of his complaint to be substantiated. Fortunately, the complainant was fully aware of the role of our office; as many people are not, it is most important that public bodies ensure that their section 8(1)(c)(iii) obligation is met when they respond to a request.

SECTION 10: EXTENDING THE TIME LIMIT FOR RESPONDING

7 No-copying Edict Sidetracks Access Request

A fired employee complained she had been the victim of discrimination. Her public body employer told her that her grievance didn't meet the requirements for consideration under the public body's internal human rights complaint process. The woman appealed this decision and in addition made an access to information request for all internal communications about her.

The human resources department told her that in order to consider her appeal it would need access to the conflict resolution program coordinator's file, which could not be copied while an appeal was underway. The department gave her the option of deferring her appeal until completion of the access to information process, or putting the access request on hold while the appeal took place. She chose the latter option.

After the appeal had been dealt with, the public body began processing the access request. The woman later complained to us about the length of time the public body was taking to respond. After factoring in the period of time the request had been put on hold, the public body purported to exercise its right under section 10(1) of FIPPA to extend the response period by 30 days, citing the large number of records involved. Once this time was up, the public body did not, as required under section 10(2), request a further time extension from us. The severed records were released in batches several weeks later.

We found the complaint to be substantiated, and not only because the public body had exceeded the response time it had calculated after factoring in the time the access request was put on hold. FIPPA does not authorize public bodies to decline to copy records requested under FIPPA or to require access requests to be put on hold. The public body acknowledged that the employee should not have been forced to choose whether or not to put her access request on hold; it also assured us it would not in future prohibit the copying of any records requested under FIPPA.

The public body suggested, however, that FIPPA be amended to enable an access request to be put on hold on agreement between a requester and public body. Its reasoning was that doing so might provide an opportunity for a greater number of records to be released in circumstances where certain records were not likely to be available during the statutory period allowed for a response. Although permitting a hold in such circumstances might occasionally work to the benefit of a requester, such an amendment might also create the risk of abuse that outweighs the inconvenience of resubmitting an access request to obtain any outstanding records.

SECTION 12: CABINET AND LOCAL PUBLIC BODY CONFIDENCES

8 Municipality on Solid Ground withholding Consultant's Report

A reporter asked us to review a municipality's decision to withhold from him a copy of a consultant's report released to council in an *in camera* meeting.

Section 12(3)(b) of FIPPA states that the head of a public body may refuse to disclose information that would reveal the substance of deliberations of a meeting of its elected officials if legislation authorizes holding the meeting in the absence of the public (i.e., an *in camera* meeting). The municipality stated that the consultant's report was reviewed by council in an *in camera* meeting and releasing the report would reveal the substance of council's deliberations.

Section 12(3)(b) requires that three tests be met. The municipality must establish that it has legislative authority to hold an *in camera* meeting, that the *in camera* meeting has been properly held and that revealing the disputed records would reveal the substance of deliberations of the meeting. The municipality provided our office with a copy of the meeting minutes and a copy of the consultant's report.

The municipality was able to establish that section 90(1) of the *Community Charter* authorized it to hold an *in camera* meeting; that the *in camera* council meeting minutes confirmed that the meeting was properly held; and that the contents of the report were deliberated on by council and releasing the report would enable the substance of deliberations to be inferred.

The reporter accepted our conclusion that the municipality was authorized to withhold the consultant's report under section 12(3)(b).

9 Man Demands Minutes of School Board Meetings Discussing School Closure

A man concerned about the scheduled closing of the school in his neighbourhood asked the School Board to give him all the information used to make the decision. In his request for the records, he indicated his understanding that several discussions on which schools should be considered for closing had been held at *in camera* (not open to the public) meetings.

The School Board responded by providing a copy of a consultant's report that had been prepared to assist in the decision-making process, but withheld the records of the meetings, citing the provisions of the *School Act* permitting meetings to be held *in camera*. The man pointed out that the School Board's own policy required that "a record of in-camera meetings shall be provided to the public". He then wrote to our office expressing his belief that there were other records that he should have received and that the School Board had not conducted an adequate search for these records.

Section 6 of FIPPA requires public bodies to "make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely." Public bodies must search for and identify which records are responsive to a request before applying any FIPPA exceptions to disclosure of information. After we contacted the School Board to clarify this responsibility, the board conducted a further search and identified three meetings at which the subject matter of the complainant's request had been discussed.

Section 12(3)(b) of FIPPA allows public bodies to refuse to disclose information that would reveal the "substance of deliberations" of a meeting of a local public body's governing body if an Act authorizes the holding of the meeting in the absence of the public (*in camera*). In this case, the *School Act* clearly authorized holding meetings *in camera* and the meetings were properly held *in camera*. The School Board regularly published a "Notice of *In Camera* Meeting Held", which showed the date of the meeting and the topics on the agenda. This document was included with the notices of general meetings held and satisfied the requirements of the School Board policy. However, it did not satisfy all the requirements of FIPPA for the applicant's request.

Section 12(3)(b) protects discussion at *in camera* meetings to allow for frank and open debate before decisions are made. It does not, however, protect information such as the identities of those who attended a meeting, the time, date and location of the meeting, and, in most cases, the identity of the subjects under discussion at the meeting.

After we explained this requirement, the School Board released to the complainant the responsive portions of the minutes from the three meetings, with the substance of deliberations withheld under section 12(3)(b). It also released certain attachments to the minutes that had been provided to the board members to assist them in their decision-making.

SECTION 13: POLICY ADVICE, RECOMMENDATIONS OR DRAFT REGULATIONS

10 Water District's Aquifer Study Not Exempt as Advice to a Public Body

A resident of a water district was concerned that new housing developments risked depleting the aquifer that supplied the community to the point that future water supplies might be jeopardized. Wanting to obtain more information to determine whether his concerns were justified, he asked the district for a copy of a hydrogeological study of the aquifer it had commissioned some time previously. When the district responded that it had decided to withhold the study under sections 13 and 17 of FIPPA, the resident asked us to intervene, as he felt that the contents of the study were a matter of public interest and the public had a right to know what it said.

On reviewing a copy of the study provided to us by the district, we found it largely consisted of a detailed analysis of the structure of the aquifer. In addition, the study identified potential new well sites for accessing the underground water supplies.

Under section 13 of FIPPA, the head of a public body may refuse to disclose to an applicant information that would reveal advice or recommendations developed by or for a public body. However, section 13 also provides that a public body must not refuse to disclose information such as factual material and feasibility or technical studies relating to projects of a public body. Under section 17, a public body may refuse to release to an applicant information the disclosure of which could reasonably be expected to harm the financial or economic interests of a public body.

The district accepted our view that, insofar as the study was both technical and in large part factual, section 13 required the disclosure of the study, subject to any severing that might be reasonable under section 17. The district's primary concern, which lay behind its reluctance to release the study, was that publicly revealing the location of potential well sites might benefit competitors seeking access to the same water resources, to the detriment of the district. The risk of harm being both real and substantial, we concluded that the district's reliance on section 17 regarding this particular information was reasonable.

When we conveyed this conclusion to the resident, he told us he had no need to know the locations of potential well sites, so the district severed this information and gave him the balance of the study.

SECTION 14: LEGAL ADVICE

11 ICBC Severing Meets Litigation Privilege Test

A lawyer made an access request to the Insurance Corporation of British Columbia for the claim file of a client who had been involved in a motor vehicle accident. ICBC provided a copy of the file but withheld a considerable amount of information under sections 14, 17 and 22 of FIPPA.

ICBC maintained that it had appropriately applied the section 14 exception because the material in question consisted of communications between ICBC and its solicitors or records created in contemplation of litigation. Under the common law, a public body claiming litigation privilege must prove that the dominant purpose for creation of the record was to conduct, assist with or advise upon litigation under way or in reasonable prospect at the time of its creation. On reviewing the records, we were satisfied that this test had been met.

ICBC also made a persuasive case that the information it withheld under section 17 was information, such as reserve information (the estimated maximum cost of settling a claim), that, if disclosed, could harm ICBC's financial interests relating to the settlement of the claim. The information to which ICBC applied section 22 is comprised of the addresses, telephone numbers, insurance information, employment information and other information of third parties and was also justifiably withheld.

SECTION 15: DISCLOSURE HARMFUL TO LAW ENFORCEMENT

12 Narrowed Request Gains Limited Access to Police Chief's Work Calendar

A police department denied a request for access to the work calendar of a former police chief under section 15 of FIPPA, taking the position that releasing the calendar could harm a law enforcement matter. The department also refused access to the records on the basis that disclosure of information in the calendar would invade the chief's personal privacy. The applicant asked us to review this decision.

With the assistance of our office, the applicant narrowed his request to exclude any investigative matters and any personal appointments. Following the narrowing of the request, the police agreed to release a severed version of the calendar. The applicant was satisfied with this outcome. Under section 4(2) of FIPPA, if information can reasonably be severed (or removed) from a record, an applicant has the right of access to the remainder of the record. In this case the public body should have removed the personal information and law enforcement information and disclosed the remainder of the calendar rather than simply denying access to the whole record.

SECTION 16: DISCLOSURE HARMFUL TO INTERGOVERNMENTAL RELATIONS OR NEGOTIATIONS

13 Concern about Provincial-Federal Relations Constrains Ministry Response

In response to a request for records related to offshore oil and gas exploration, the Ministry of Energy, Mines and Petroleum Resources released a small amount of information but withheld the majority of records under section 16 of FIPPA in the belief that release would adversely affect intergovernmental relations with the federal government. The ministry also withheld information under section 17 on the basis that some of the information could harm the financial interests of the provincial government.

After reviewing the records at issue, we asked the ministry to consult with the federal government to re-examine its assumption regarding harm to intergovernmental relations. The ministry did so and released additional records but continued to rely upon section 16(1) of FIPPA as authority to withhold a portion of the information. Although the applicant was not entirely satisfied with the result, he accepted it after we told him that the Commissioner had previously decided a similar matter, and in that case had upheld the ministry's decision to deny access to similar information based on section 16 of FIPPA.

SECTION 17: DISCLOSURE HARMFUL TO THE FINANCIAL OR ECONOMIC INTERESTS OF A PUBLIC BODY

14 Release of Economic Model Could Harm Public Body's Negotiating Position

An applicant asked a public body for a copy of an "electronic model" that was used during the development of a public sector infrastructure project, to make comparisons between the costs of a project utilizing the traditional "design/build" contracts and the costs of the same project utilizing "design/build/finance/operate" contracts, which are characteristic of a public private partnership. The public body refused to disclose the electronic model, saying it fell under FIPPA's section 17 exception to the right of access to information.

After initially reviewing the file, we suggested to the applicant that the electronic model might fit the definition of a "computer program". A computer program is not a record, according to Schedule 1 of FIPPA, and would not be subject to FIPPA. The electronic model, while it could be accessed using a common software application, also contained additional proprietary applications created by a third party. Rather than simply being an electronic file that could be opened and viewed on a computer, the electronic model was described by the public body as an application that could receive input in the form of data and perform calculations to enable users to make financial comparisons.

Under section 17, a public body may refuse to release information the disclosure of which could reasonably be expected to harm the financial or economic interests of a public body. The public body argued that electronic models like the one requested by the applicant also create benchmarks against which proposals are evaluated. The public body claimed that it was reasonable to expect that the disclosure of the electronic model could provide proponents with the ability to estimate more accurately the value of future projects and this could compromise a public body's evaluation process and cause harm by undermining the public body's negotiation position.

We concluded that the electronic model was likely not subject to FIPPA but if it was, the public body's reliance on section 17 to withhold the model was reasonable.

In an effort to resolve the dispute, the public body provided the applicant with a paper printout of the model. The applicant did not consider the printout satisfactory but did not pursue the review any further.

SECTION 21: DISCLOSURE HARMFUL TO THE BUSINESS INTERESTS OF A THIRD PARTY

15 Patient Challenges Decision to Discontinue Drug Coverage

A man was dismayed to learn out that the Ministry of Health was discontinuing coverage of a drug prescribed by his doctor. When he questioned the change, he was told that a rigorous literature review by a panel of health care professionals had determined there was insufficient evidence to show that people taking the drug experienced any real benefit.

Not pleased at the prospect of paying several thousand dollars a year for a drug his doctor considered a beneficial treatment, the patient requested access to the literature review so he could have a chance to rebut whatever conclusions it contained. The ministry denied access to the records under section 21 of FIPPA on the basis that there was proprietary information in the scientific studies that were reviewed.

Our own review of the records made clear that much of the information in question could be found on the internet or at any university library and was now in the public domain whether or not it had once been proprietary. Once we brought this fact to the ministry's attention, it reconsidered its position and released to the applicant the literature review in its entirety.

SECTION 22: DISCLOSURE HARMFUL TO PERSONAL PRIVACY

16 Opinion about Applicant Belongs to Applicant

A public body disclosed to an applicant a severed copy of a letter the public body received about the applicant. The released portion identified the author of the letter, but the author's opinions about the applicant were severed. The applicant asked our office to review the public body's decision to withhold that information.

As a result of our office's involvement, the public body wrote a new decision letter indicating to the third party (the author of the letter) that it intended to release the entire letter to the applicant. The third party objected on the ground that he had provided it in confidence to the public body. He argued that section 26 of the *Foresters Act* and sections 21, 22(2)(e), 22(2)(f), 22(3)(g) and 22 (3)(h) of FIPPA all applied.

Section 26 of the *Foresters Act* says that a person who obtains information while carrying out an investigation under section 24 of that Act must not disclose the information to anyone except for the purpose of carrying out a duty under the Act, the bylaws or the resolutions as required by law. We concluded that section 26 of the *Foresters Act* did not assist the third party, as the senior manager was not the Registrar for the Association of BC Forest Professionals and the third party's discussions with

the senior manager were not meant to result in an investigation, under section 24 the *Foresters Act*, of the conduct of the applicant. As well, the *Foresters Act* does not contain a clause providing that it overrides FIPPA.

The letter's author couldn't provide objective evidence that the release of the information would likely harm significantly the competitive position or interfere significantly with the negotiating position of the third party or that it would result in undue financial loss to the third party. Nor did section 22 of FIPPA apply. The letter's author couldn't show that he would be exposed unfairly to financial or other harm if the letter were disclosed, nor that the applicant was seeking personal recommendations or evaluations about the third party. Nor was the letter a personal recommendation or evaluation of the applicant, so section 22(3)(h) of FIPPA didn't apply. The letter was released.

17 Relative of Murder Victim Seeks 50-Year-Old Records of Police Interviews

A man asked a police department for records related to the murder more than 50 years ago of an extended family member, which the police had solved within months of the killing.

The police department denied access to all of the records under section 22(3)(b) of FIPPA, which provides that if personal information was compiled as part of an investigation into a possible violation of law, its release is presumed to be an unreasonable invasion of privacy.

After reviewing the records and discussing them in general with the applicant, we determined that he was only interested in any interviews that police might have conducted with family members or co-workers of the victim, as well as interviews with the murderer. We discussed the narrowed request with the department, and it then released several records of this type after reconsidering the age of the file, the relatively low sensitivity of the information in the interviews and the fact that most if not all of the people involved had likely died long ago. The applicant was satisfied with this resolution to the matter.

18 Innocent Buyer of Grow-op House Blindsided by Building Inspection

A city received a report from BC Hydro (pursuant to section 19 of the *Safety Standards Act*) to showing higher than normal power consumption at a residential address. The request led the city to believe the home had been used for a marijuana grow operation. Several months passed before the city was in a position to act on that information. In the meantime, the home was sold. The new owner was somewhat surprised to be informed later that the city would be conducting a building inspection.

The inspection revealed alterations to the building consistent with a grow operation. The defects raised safety concerns, requiring the city to condemn the home until the deficiencies were corrected, at considerable expense to the new owner. Suspecting that

the previous owner had known about the grow operation and had failed to disclose this important information in the sales agreement, the new owner asked the city for all records pertaining to the building inspection. In response, the city withheld only the hydro report, arguing its release would result in an unreasonable invasion of the privacy of the BC Hydro customer under section 22 of FIPPA.

During mediation, it became clear that the applicant simply wanted to know whether the previous owner was the hydro subscriber at the time of the grow operation. As the BC Hydro record did not contain the name of the previous owner, the city agreed to give the applicant written confirmation that the previous owner was not the hydro subscriber at the time of the grow operation, thus resolving the matter.

19 Tempers Flare over Building Encroachment on Parkland

The renovation of a rural house left the neighbours up in arms when it was discovered that a corner of the building encroached on parkland and blocked a trail to the beach. Several people wrote to the ministry administering the park to complain about the infringement and demanded that the owner of the house relocate the portion of the structure that had strayed outside her property. She responded that the encroachment was entirely accidental.

Upset about the letter-writing campaign, the woman asked the ministry for copies of the correspondence. The ministry gave her copies of emails with the identities of the authors removed, and withheld several handwritten letters in their entirety on the basis that the handwriting would reveal the identities of the writers and that some of the complainants had specifically asked that their identities be kept confidential. Consistent misspelling of her name in the emails led her to believe that most had been written by one person, and she assumed the same to be the case with the handwritten letters. Believing she was the target of a malicious campaign by one or two people, she asked us to review the ministry's decision.

We concluded that the decision was justified under section 22(1) of FIPPA. First, section 22(3)(b) provides that a disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if the personal information was compiled and is identifiable as part of an investigation into a possible violation of law. This provision includes the investigation of municipal bylaw infractions. In addition, under section 22(2)(f), a decision made under section 22(1) must take into account whether the personal information has been supplied in confidence, and the content of the letters led us to believe that this was generally so. Finally, in a small rural community, disclosure of handwritten letters might reveal the identities of their writers almost as surely as would the release of their names.

After reviewing all of the letters, we confirmed to the applicant that the differences in script among the letters were so distinct that it was clear to us that each letter had been written by a different person. We also obtained from the ministry a commitment

to summarize the contents of the letters for her, as they were about her and summaries could be prepared, as required by section 22(5), without disclosing third parties' identities. As she could imagine the gist of the contents of the letters and was interested only in knowing who wrote them, she declined this offer.

SECTION 30: PROTECTION OF PERSONAL INFORMATION

20 Laptop Theft Shows Need for Security Policy for Portable Storage Devices

A laptop containing sensitive medical information was stolen from a public body's contracted agency. The personal information of 53 families on the laptop was neither encrypted nor password protected. The public body owning the laptop reported the theft to the police and sent reminders to staff about the physical security policies of the workplace and building.

On assessing the risk associated with the breach, the public body correctly determined that it needed to notify the affected parties and did so. It then notified our office as well. In addition to recommending improvements to future notification letters, we examined and commented on the public body's security policies.

The public body already had prevention strategies in place, including privacy breach guidelines. We recommended that it also incorporate the four key steps for responding to privacy breaches, posted on our website at http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf

We also recommended further prevention strategies to safeguard against future breaches, including

- conducting annual privacy audits;
- entering information and privacy management confidentiality agreements with contractors;
- conducting privacy, security and confidentiality training; and
- developing portable storage device security policies.

Security on portable storage devices is an important safeguard in the prevention of privacy breaches, and we recommend that all public bodies adopt the following standards to ensure compliance with the requirement under section 30 of FIPPA for reasonable security arrangements for the protection of personal information:

(1) Storage of personal information on local hard drives and portable storage devices should be generally prohibited. Staff should be required to access personal information only through secure connections to a secure server.

(2) Storage on local hard drives and portable storage devices should only be permitted when absolutely necessary. If such storage does occur, policy should require that only the minimum amount of personal information needed be stored and only for the minimum amount of time necessary.

(3) Personal information must be immediately deleted after use or stored on a secure network drive as soon as possible.

(4) Personal information stored on a local hard drive or portable storage device must be encrypted; password protection is not sufficient.
(5) Laptops must be cable locked to desks during use and must be stored inside a locked cabinet or desk when not in use.
(6) While in transit, laptops must not be left unattended.

SECTION 33.1: DISCLOSURE OF PERSONAL INFORMATION INSIDE OR OUTSIDE CANADA

21 Survey Plans Go Awry with Disclosure of Client Names to US-based Service Provider

A manager at a public body contracted a US-based service provider to conduct client surveys and later emailed the personal information of nearly 10,000 clients to the US service provider to meet its need for survey participants. The service provider then mailed the clients a letter inviting them to visit a US-based website to complete the survey.

The manager had unwittingly breached section 33.1(1) of FIPPA, which defines the limited circumstances under which public bodies may disclose personal information outside Canada. On discovering the breach, the public body reported it to us using the Privacy Breach Reporting Form on our website. We then worked with the public body to address the breach and mitigate its effects.

The public body immediately had the US-based website shut down and ensured that all personal information sent to the US-based company was destroyed. The public body then evaluated the risks associated with the breach, determined that affected individuals needed to be notified, and wrote to them. The notification letter summarized the survey program and explained the public body's obligations under FIPPA, how the public body had breached those obligations and the steps taken by the public body to contain the breach and minimize the risk (by destroying the data and shutting down the website). It also provided a contact name and phone number of an employee at the public body who could answer questions about the breach, as well as contact information for our office.

SECTION 33.2: DISCLOSURE INSIDE CANADA ONLY

22 Health Authority Demands Proof of Law Enforcement Status

A conservation officer sent an email to a health authority requesting information from a health inspector who had initially attended the scene of a raw sewage spill. The conservation officer was conducting a separate investigation under section 6(4) of the *Environmental Management Act*, which makes it illegal to "introduce waste into the environment in such a manner as to cause pollution". The health inspector refused to provide the information directly and told the conservation officer to submit an FOI request.

The conservation officer did so, but when he received the records much of the personal information, in the form of names and contact information of individuals, had been withheld under section 22 of FIPPA. Section 22 requires public bodies to not disclose personal information of a third party if the disclosure would be an unreasonable invasion of the third party's personal privacy. The conservation officer then asked our office to review the health authority's decision, stating that the health authority had the discretion to disclose the information sought under section 33.2(i) of FIPPA.

The applicant was correct in identifying section 33.2(i) as discretionary authority for the public body to disclose the information to a law enforcement body in Canada. This section authorizes such a disclosure to assist in a specific investigation, undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. However, the onus was on the applicant to satisfy the public body that he represented a law enforcement agency in making the FOI request and that the information was being sought to further an investigation into a breach of the law.

In an effort to mediate the dispute and avoid the need for a formal hearing, we contacted the health authority and discussed the application of section 33.1(i). The health authority agreed that, if it received satisfactory documentation from the applicant describing his authority as a law enforcement officer and the investigation he was conducting, it would disclose the records in their entirety. The applicant re-submitted his request with the required information and received the records without severing.

The public body was simply being diligent in protecting personal information under its control or in its custody. The case was a useful reminder that applicants should thoroughly review their requests for records before submitting them to ensure that they have provided public bodies with all the information they require. By doing so, applicants are more likely to receive the records in a timely fashion without the need for our office's involvement.

23 Ill Worker Complains of Improper Disclosure by Employer to Hospital Visitors

A hospital worker who had been on sick leave was meeting with her manager to discuss her return-to-work plan when she fell ill and was admitted to the hospital as a patient. During her stay there, the employee received unsolicited visits from the hospital's human resources consultant and chaplain. She later complained to the hospital and then to us that the visits resulted from the improper use and disclosure of her personal information.

FIPPA restricts a public body's use and disclosure of personal information. A public body may only use personal information under three circumstances: for the purpose for which the personal information was collected or for a consistent purpose; if the individual the personal information is about has consented to its use; or for a purpose for which the information can be disclosed without consent under FIPPA. Section 33 of FIPPA

restricts disclosure of personal information to the purposes listed in sections 33.1 and 33.2. Relevant to the circumstances of the complaint, section 33.2(a) permits disclosure for the purpose the information was obtained in the first place or for a use consistent with that purpose, while section 33.2(c) permits disclosure to an employee of a public body if the information is necessary for the performance of that employee's duties.

In response to the employee's complaint, the health authority responsible for the hospital investigated the alleged breaches of privacy and produced a report with the results and a number of strategies to prevent further breaches. The health authority provided the report to our office.

Our investigation in this case determined that the employee's manager disclosed the employee's personal information by revealing the events of the back-to-work meeting to the human resources consultant. The human resources consultant used the personal information to locate the employee and visit her. Also, the employee's personal information was disclosed by an unknown person to the chaplain, who used that information for the purpose of visiting the employee.

We concluded that the manager's disclosure of the events of the return to work meeting to the human resources consultant was reasonable in the context of their work relationship. The consultant needed to know the status of the back-to-work plan. While it is likely that more personal information than absolutely necessary was disclosed, we found that it was reasonable, under section 33.2(c), to share personal information to determine what further action was required.

Our finding regarding the chaplain's visit was that there was no authority under FIPPA for her to use the employee's personal information for the purpose of visiting. The hospital determined that it was not necessary for the human resources consultant to visit the employee for the purpose of fulfilling her job duties. While our office could not confirm the chaplain's intention, it appears the nature of her visit was personal. Using personal information she collected at work for this purpose was a breach of section 32 of FIPPA, regardless of how well intentioned that use may have been.

We also concluded that disclosure to the chaplain about the employee's status as a patient and her location was a breach of section 33 of FIPPA. Our office has received numerous complaints over the years regarding unsolicited visits by hospital chaplains and it is our view that patient information should not be disclosed to chaplains without a patient's consent.

The employee's complaint was partially substantiated. The public body acknowledged the lapses in privacy protection in this case and implemented a series of privacy-related activities to address both general privacy issues and issues specific to this case. These included posters aimed at hospital staff, in-service workshops for various work groups and enhanced privacy education during new staff orientation. Satisfied with the health authority's investigation into the matter and their strategies to prevent further privacy breaches, we closed the file without making recommendations.

SECTION 75: FEES

24 Refined Calculation Reduces Fee Estimate for Engineering Records

A lawyer acting for an unnamed client made two different access-to-information requests to a regional district for information related to a major water filtration project. In both cases the regional district responded with fee estimates and requested payment of a deposit of 50% as a condition of processing the requests.

Section 75 of FIPPA authorizes a public body to require an applicant to pay a fee for

- locating, retrieving and producing a record;
- preparing the record for disclosure;
- shipping and handling the record; and
- providing a copy of the record.

Fees do not apply to the first three hours spent locating and retrieving a record, to the time spent severing information from a record or to a request for the applicant's own personal information.

An applicant may make a written request to the public body to have the fees waived. A public body may waive all or part of the fees if, in its opinion, the applicant cannot afford the fee, if the public body considers it fair to excuse the fee, or if the record relates to a matter of public interest. It is the responsibility of the applicant to demonstrate that any of these conditions apply.

The lawyer representing the applicant asked our office to review the amount of the fee estimate for each request. The applicant had not made a direct request to the public body for a fee waiver.

A public body's fee estimate is just that: an estimate. Often the public body's freedom of information analysts depend on staff in the program areas to provide them with details about where records are stored, how many records need to be searched and how long it may take to gather them up. In this case the requested records were mostly engineering records stored at the public body's head office, at the contractor's field office, at several worksites, or in offsite storage. An estimated 5,000 records needed to be searched.

In an attempt to resolve the matter once it came to our attention, the regional district went back to the engineers to try and refine the fee estimate. As a result, it was able to reduce both fee estimates, by a small amount in one case and substantially in the other. The lawyer for the applicant accepted the new estimates as reasonable and withdrew the complaints.

25 Businessman Challenges Fee Estimate for Production of Letters

A businessman who asked a public body for copies of two letters was told it would cost him $60 for an estimated 70 minutes' time. He complained to us that the fee seemed excessive for the amount of work involved.

The fee for time spent responding to the request was not merely excessive; it should not have been charged at all. When we asked the public body for a breakdown of the

calculations used to determine the fee estimate, it became clear that the estimated time for locating, retrieving and preparing the records was far less than three hours. Section 75(2) of FIPPA provides that a public body may not require payment of a fee for the first three hours spent locating and retrieving a record.

When we pointed this out, the public body responded that it was justified in charging the fee because the businessman was a "commercial applicant", not an ordinary citizen. Section 7 of the Freedom of Information and Protection of Privacy Regulation does distinguish between commercial and other applicants, setting maximum fees for charges to applicants other than commercial applicants but authorizing a charge to commercial applicants of the actual cost of providing location, retrieval and preparation services. However, section 75(2) makes clear that no such distinction applies to the first three hours' of time spent responding to a request.

In response to the public body's request for written confirmation that no applicant can be charged for the first three hours locating, retrieving and preparing records, we provided the public body with previous Commissioner's orders on the same subject matter. The public body then sent the requested records in their entirety to the applicant without charge.

26 Journalist Makes Public Interest Argument for Investigation of Self-Governing Bodies

A journalist investigating the disciplinary processes used by self-governing bodies (listed in Schedule 3 of FIPPA) to investigate and discipline their members asked one such body for a copy of all its disciplinary reports over a two-year period. The self-governing body was willing to release the requested records but for a fee that the journalist thought unreasonably high.

The journalist submitted that the public body should waive the fee because the disciplining of health professionals in B.C. was clearly a matter of public interest – a criterion to be considered for a discretionary fee waiver under section 75(5)(b) of FIPPA. The self-governing body disagreed and the journalist complained to us that its response was unreasonable.

Preliminary investigation showed that the self-governing body had calculated the fee incorrectly and had estimated too high an amount. It then agreed to recalculate the fee to a lower amount.

In an attempt to mediate the dispute, and in the interests of maximizing public accountability, we suggested a 50% fee waiver,. Both parties agreed to reduce the fees by a further 50%, the applicant paid the reduced fee, and the records were released.

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY REGULATION, SECTION 3

27 Public Body Denies Parent's Request for "Capable" Child's Medical Records

A parent who believed a public body had not provided competent medical treatment to the parent's adolescent child asked the public body for records relating to the treatment. The public body refused to grant access to the medical records without the child's authorization since the child was capable of giving consent to medical treatment under section 17 of the *Infants Act*. The minor child would not authorize the public body to disclose medical records to the applicant.

Under section 3(a) of the Freedom of Information and Protection of Privacy Regulation, a parent may exercise access rights on behalf of a child under 19 years of age if the child is incapable of exercising those rights. In this case, we concluded that the applicant did not meet the criteria of section 3(a) of the Regulation.

First, we concluded that the applicant was not acting "on behalf of" the minor child but on the applicant's own behalf as a concerned parent. The minor child was living independently and would not consent to the applicant having access to the child's medical records. Secondly, we concluded that the minor child was not "incapable of exercising" his or her own access rights under section 3(a) of the Regulation. The minor child was legally capable of appreciating and understanding the nature of his or her own actions. The minor child was also working, had a partner and was considered legally capable for the purposes of making medical treatment decisions.

Under the *Freedom of Information and Protection of Privacy Act*, ("FIPPA") the access request of a parent who does not meet the criteria of section 3(a) of the Regulation must be considered from the perspective of an ordinary arm's-length request about the personal information of a third party. Under section 22(3)(a) of FIPPA, the disclosure of personal information about the medical treatment of the applicant's minor child would be presumed to be an unreasonable invasion of the child's personal privacy. This information could be disclosed under section 22(4)(b) of FIPPA if there were compelling circumstances affecting the child's health or safety. In this case, however, there were no compelling circumstances that would permit the public body to disclose the medical records. "Compelling circumstances" normally connote a health emergency that would preclude obtaining an individual's consent to the release of the individual's personal information. In this case, the minor child's medical condition did not constitute the type of medical emergency that would preclude obtaining the child's consent to disclose this information.

We concluded that, without the authorization of the applicant's minor child, the decision of the public body to refuse access to the minor child's medical records was correct as the applicant was not entitled to exercise her minor child's access rights under section 3(a) of the Regulation. The applicant did not consider this result satisfactory but declined to request an inquiry.

3.2 FIPPA Orders

28 Order F07-10: The Board of Education of School District No. 75 (Mission)

In 2004, The Board of Education of School District No. 75 (Mission) began using the "Gallup Teacher Insight Assessment", an on-line computer-based assessment tool, developed and administered in the United States, to screen applicants for teaching positions. In 2005, the British Columbia Teachers' Federation and the Mission Teachers' Union complained to us that the Board's collection of personal information through the Assessment contravenes sections 26, 30, 30.1 and 32 of FIPPA. The complainants also alleged the requirements of section 30.1(a) were not met because the consent to storage and access outside Canada was not voluntary and did not meet the prescribed requirements for consent.

The Information and Privacy Commissioner found that the collection of personal information through the Assessment was not expressly authorized by or under an Act, but that it did, with the exception of social insurance numbers, relate directly to the Board's recruitment process for new teachers under section 26(c) and is necessary for that process. He also found that the Board made reasonable security arrangements for the protection of the personal information under section 30.

The Commissioner then found that the electronic form of consent was sufficient and there was no evidence that the consents were not voluntary. The use of the personal information for screening new applicants was consistent with the purpose for which it had been obtained under section 32(a) and also met the consent requirement under section 32(b).

29 Order F07-21: Public Guardian and Trustee for British Columbia.

A woman requested access to records related to her deceased mother in the hands of the Public Guardian and Trustee, which had been the mother's committee for some years prior to her death. The daughter referred to a dispute over the validity of her mother's will and said she needed the PGT's records to assist her in determining her mother's "testamentary capacity". She argued she had authority to obtain them under section 3(c) of the Freedom of Information and Protection of Privacy Regulation, which permits the "nearest relative or personal representative" to access records "on behalf of" a deceased person. The PGT refused access to the records on the ground that the applicant was acting in her own interests rather than on behalf of her late mother's estate.

The Adjudicator found that the applicant could not make a request for access to her deceased's mother's records held by the PGT because the PGT was still the committee. The adjudicator concluded that, as long as an individual has a committee, then, deceased or not, section 3(b) of the Regulation applies and only the PGT may exercise the personal information rights accorded under FIPPA on behalf of the individual.

(Section 3(b) of the Regulation allows an individual's committee to act on behalf of the individual.) The adjudicator found that the PGT was required to refuse the applicant access to the records except for those portions which contained the personal information of the applicant and the disclosure of which would not unreasonably invade the personal privacy of a third party.

30 Order F08-03: Ministry of Public Safety and Solicitor General

The applicant, the CBC, sought access to reports made under section 86 of the *Gaming Control Act* from casino operators relating to suspected or actual criminal activity in casinos. The ministry refused access to any information, citing sections 15(1)(a) and (l) and section 21 of FIPPA. The Information and Privacy Commissioner found that the ministry was not authorized by section 15 or required by section 21 to withhold access to the records but was required under section 22 to withhold some third-party personal information in them. The Commissioner ordered the ministry to sever the personal information and release the remainder of the records to the applicant within 60 days.

In Order F08-07, a decision flowing from Order F08-03, the third-party casino operators requested further consideration of one aspect of the section 22 guidelines in Order F08-03. The Commissioner decided to permit further submissions on that issue. In the meantime, he said, the ministry had to disclose the section 86 reports, as ordered in Order F08-03, with some exceptions. The exceptions were: information required to be withheld according to the guidelines in Order F08-03; and the names of casino employees acting in a professional or employment capacity, the disclosure of which remained unresolved pending further consideration of section 22 arising from Order F08-03. The Commissioner had not dealt with the remaining matter as of the end of the fiscal year.

31 Order F07-08: Ministry of Environment and Sierra Legal Defence Fund

An environmental group wanted to see records that showed if any company or municipality had discharged pollutants in breach of the *Waste Management Act*. It wanted to produce its own version of the "BC Environment Non-Compliance List" that the Ministry of Environment had stopped publishing. The ministry agreed to produce the records for a fee it estimated at $24,060.

The environmental group asked that the fee be waived because the information was about the environment and, it argued, related to a matter of public interest. During mediation on the matter with our office, the ministry, after reviewing how much work would be needed to get records from about 5,000 files, raised its fee estimate to $172,947. It guessed that 5% of the records were about a public interest matter and waived 5% of the fee.

The Adjudicator reviewed the legal requirements of section 75 of FIPPA for charging and waiving fees and the steps the ministry had taken in this case. She accepted the ministry's estimate of the number of records but not its estimate of the costs to produce them. Nor did she accept the ministry's guess of how many records were related to a public interest matter, as it had not examined a sample volume and range of the records before deciding on a fee waiver based on public interest. She required the ministry to look at the records again, make another decision about fees and the waiver request, and give the applicant proper reasons.

The Adjudicator also found that there will be cases where it makes sense for an applicant to ask for a fee waiver and request access to records at the same time. This was such a case. The public body should have responded to the group's first fee waiver request. Both parties were admonished for their lack of communication.

32 Order F07-22: British Columbia College of Chiropractors

After complaining about a chiropractor to the College that regulates that profession, a patient asked the College for a copy of the letter the chiropractor wrote in response to her complaint. The College refused. The Adjudicator ordered the College to give her access to the letter.

Much of what was in the letter was the patient's own personal information, such as the chiropractor's diagnostic comments about her made at the time of treatment. FIPPA entitled her to that information and there were no reasons to withhold it from her. Although the letter contained some personal information of the chiropractor ("occupational history" under section 22(3)(d) of FIPPA), the Adjudicator found that disclosure would not be an unreasonable invasion of personal privacy. The letter was not given to the College on a confidential basis. The Adjudicator also questioned the College's blanket policy of not disclosing such responses to complaints. The benefit of public scrutiny of self-regulating professions weighed in favour of disclosure.

4 CASE SUMMARIES: PIPA MEDIATIONS AND ORDERS

4.1 PIPA Mediation Summaries

SECTION 5: POLICIES AND PRACTICES

33 Dating Service's Privacy Policy Bad Match with PIPA Requirements

Section 5 of PIPA requires every organization that is subject to PIPA to develop and follow the policies and practices needed for compliance with PIPA requirements for the protection of personal information. For the most part, organizations have been conscientious about meeting these obligations, although lawyerly zeal in protecting a corporate client's every conceivable zone of vulnerability occasionally runs counter to the letter and spirit of PIPA.

Such was the case when an online dating service based in BC posted its privacy policy on its website. Our office initiated an investigation after noting questionable language in the privacy policy, one section of which contained the following wording:

"By using this service, you agree and consent that [the organization] may at its sole discretion and without your consent and without notifying you (whether before or after the disclosure) disclose your personal information to any person at any time and for any purpose, including, without limiting the generality of the foregoing, in any one or more of the following instances:" – followed by most of the list of provisions in section18 of PIPA authorizing disclosure of personal information without consent.

Although section 18 enumerates several situations in which disclosure without consent is authorized, our concern was the breadth of the powers the organization was bestowing upon itself – in short, disclosure to anybody for any purpose. Section 17 of PIPA places strict limits on the disclosure of personal information – most notably that it can only be disclosed for purposes that a reasonable person would consider appropriate in the circumstances.

On hearing our concerns, the organization and its lawyer agreed to amend the wording of its policy regarding disclosure of clients' personal information. We also identified two other paragraphs in the privacy policy containing troublesome wording and collaborated with the organization to create acceptable alternative wording.

34 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 PIPA 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.

SECTION 7: PROVISION OF CONSENT

35 Laser Tag Business Can Collect Photo ID, but Security Needs Upgrading

A man took a group of 12- and 13-year-old boys to play laser tag, a game played in semi-darkness in which the object is to accumulate points by making "hits" on the opposing team with laser guns. Before playing, participants enter their contact information, i.e., birth date, gender and email address into a company computer. Once the data is collected, the participants photograph is taken and he/she is issued a "player card" containing his/her real name, code name, photo and a bar code. At the completion of the game, the kids insert their player card into the company computer and they receive a final score.

After they finished, the man picked up some cards discarded by previous players. When he inserted them into the computer, he was able to access each player's personal information. This disturbed him, and he made his concerns known to the organization. When he didn't receive a satisfactory response, he filed a complaint with our office, saying he was concerned about both the collection of personal information of minors (especially their photographs) without parental consent and the opportunity for unauthorized access to personal information on the organization's database.

The organization told us all players are required to complete a liability waiver for insurance purposes and to obtain emergency contact information. The organization added that it uses other demographic information for marketing analysis to determine where its clients are coming from and their typical ages and gender. Photos were

introduced to curtail incidents of vandalism, bullying and assaults. The perpetrators usually did not carry identification and provided false information when they logged into the game. Since the inception of photos the incidence vandalism, bullying and assaults has declined significantly.

During the mediation process, the organization increased signage explaining the reasons for the collection of the information. They restricted the amount of information it collected to the amount necessary to conduct their business. Finally, access to information on the player card was restricted.

PIPA provides that the guardian of a minor may give or refuse consent to the collection, use and disclosure of personal information of a minor if the minor is incapable of exercising that right.

36 Student Objects to University's Requirement for Insurance Information

A graduate student objected to a requirement at her university for mandatory enrolment in a medical/dental insurance plan administered by the Student Society. The cost of this coverage was included in student fees collected by the university. Students who already had similar insurance could, within a limited time, opt out of the mandatory plan by submitting a waiver form, together with proof of similar coverage showing the name of the existing insurance provider and the policy number, at the Student Society offices or by completing an on-line form and attaching scanned documentation to the electronic submission.

The student objected to the requirement to provide supporting documentation. When she attempted to use the on-line waiver, the form was rejected because the documentation was missing. She complained to the Student Society, but it became involved in internal difficulties and communication with the student ceased. Frustrated, she complained to us about what she considered an unreasonable demand for information and about the mandatory requirement for all students to carry extended health and dental insurance.

The complainant argued that the Student Society should have arranged to make this benefit available to all students and to let each student choose whether or not to take advantage of the offer. We confirmed that the benefit program was a program of the Student Society, not of the university. The Student Society was a registered non-profit society under the *Society Act* and had been properly designated under the *University Act*. By a large majority vote, the membership of the Student Society had approved the resolution to implement the mandatory health/dental insurance program. Under section 27.1 of the *University Act*, the university was obligated to collect the student fees as approved by the Student Society.

Since students were required to have extended health insurance, the question was whether the Student Society could require students to disclose the company name and policy number of any existing insurance in order to opt out of the mandatory plan.

Section 7 of PIPA states that organizations must not, as a condition of supplying a service, require individuals to consent to the disclosure of their personal information beyond what is necessary to provide the service. Section 11 further limits the collection of personal information to purposes that a reasonable person would consider appropriate in the circumstances. Here, the service being provided was the ability to opt out of the mandatory program and thereby avoid the corresponding fees. The purpose of collecting the insurance company name and policy number was to determine the student's eligibility for opting out.

An insurance policy number identifies the name of a particular policy, usually a group plan. It provides no links to the individual's medical history or to records of claims. These types of information may be accessed by an individual certificate number, which was not being collected. The website for the company providing the insurance program for the Student Society included the statement: "Once we confirm coverage, we DO NOT retain any confirmation documentation that you provide to us." We concluded that, in view of these relevant circumstances, a reasonable person would not consider the collection of an insurance company name and policy number to be "beyond what is necessary to provide" the service of opting out of the otherwise mandatory program and would consider requiring proof of existing coverage "appropriate in the circumstances".

SECTION 8: IMPLICIT CONSENT

37 Disability Insurance Renewal Raises Medical Information Disclosure Concern

A woman who worked at a medical office complained that a financial services organization had disclosed her personal information, without her consent, to her employer and had not made reasonable security arrangements to protect her personal information.

Years earlier, the employer had purchased disability insurance for its employees from the financial services organization. The premiums were paid by the employer, which owned the policy, and the employees were the beneficiaries. Attached to the original policy was an amendment listing the exclusion to the insurance coverage with regard to the employee who complained to us. The exclusion can be characterized as a general disorder, described in generic medical terms and based on the personal health information submitted by the employee to the organization.

The incident she complained about occurred during the policy renewal process. The renewal application required information from both the employer and the employee. The organization, conscious of the need to guard the employee's personal information under PIPA, asked the employer to fill out his information and sign the renewal application before the employee was asked to update her personal information, thus ensuring the employer did not see the information submitted by the employee. The organization put the signed form in an unsealed envelope with an addressed return envelope and gave it to the employer to pass it on to his employee.

The employee's first complaint was that the organization disclosed the amendment form, which contained health-related personal information, to the employer by including it in the renewal application package. While PIPA limits the circumstances in which an organization may disclose personal information, the legislation also recognizes that there needs to be a balance between the protection of personal privacy and the need for organizations to collect, use and disclose personal information for reasonable purposes. Section 8(2) of PIPA states that an individual who agrees to sign up for insurance, not as the applicant but as a beneficiary, implicitly consents to the collection, use and disclosure of his or her personal information for the purpose of providing insurance coverage. Our office found that the organization's disclosure of the personal information on the amendment form to the employer was authorized by PIPA.

SECTION 10: REQUIRED NOTIFICATION FOR COLLECTION OF PERSONAL INFORMATION

38 Optometrist's Patient Balks at Request for Date of Birth

A woman phoned to book an appointment for an eye examination at an optometrist's office where she had not previously been a patient. During the booking of the appointment, she was asked for her date of birth but she refused to provide this information. The office booked the appointment without collecting the date of birth but later, on a subsequent call, again asked for her date of birth. When she complained about this, she was told that she didn't have to provide her date of birth but would nevertheless be asked for it every time she called the office. Feeling that this amounted to unreasonable harassment, she cancelled her appointment and wrote a formal letter of complaint to the optometrist's office.

In its written reply, the office explained that it uses a patient's name and date of birth to confirm the patient's identity. As several people in its database had identical names to that of the complainant (not "Mary Smith" but equally common), cross-referencing a date of birth to the name helped ensure that the office did not share patient information with an incorrect patient. Dissatisfied with this explanation, the woman then brought her complaint to our office.

Section 10 of PIPA requires an organization to disclose the purposes for which it is collecting information on or before collecting the information, unless the purpose would be obvious. The information collected must be only that which is appropriate to fulfil those purposes (section 11), and the organization must not require an individual to consent to the collection of information beyond what is necessary as a condition of supplying a product or service (section 7).

In this case, it wasn't clear what explanation the optometrist's office provided to the complainant for requesting her date of birth at the time the appointment was booked; however, the office did provide an explanation in its letter to the complainant in response to her letter. In the course of our investigation, a doctor at the optometrist's

office explained that clear identification of the patient, while it may be reason enough for requiring date of birth, is not the only reason for asking for this information. Optometrists who opt out of the Medical Service Plan fee billing guidelines are required by law to quote fees before providing services to patients. Under MSP, patients under 19 years of age have full fee coverage, those 65 and over have partial coverage and those aged 19 to 64 have none. Accordingly, it is necessary to know a patient's age to quote the correct fee. Moreover, as certain diagnostic tests and treatments are age-dependent, being aware of a patient's age may be critical to ensuring appropriate health care.

Under these circumstances, we concluded that the collection of date of birth information was appropriate and that the complaint was not substantiated.

SECTION 11: LIMITATIONS ON COLLECTION OF PERSONAL INFORMATION

39 Press Questions Housing Society's Drug-testing Policy

Residents of subsidized housing operated by a non-profit society had to sign a tenancy agreement requiring them not to engage in any criminal act – including drug-related criminal activity – in the facility. Following the appearance of newspaper reports suggesting that the society was implementing a new mandatory drug testing policy for all its housing tenants, we decided to initiate an investigation. If the reports were true, the policy might be in violation of PIPA's section 11 requirement that an organization collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

A conversation with the society's executive director and a review of documents she provided at our request satisfied us that the media reports were inaccurate. Among its activities, the society operates programs (employment readiness, for example) that require abstinence from drugs and alcohol. Although the society makes consent to mandatory random drug testing a precondition for participation in the programs, the consent is voluntary in the context that entry into the programs is voluntary. Thus it was true that the society conducted random drug testing of program participants but not true, as the media reports had implied, that all housing tenants were subject to testing.

Some tenants of the apartment complex run by the society had complained about the smell of marijuana in the building. This was why management felt the need to ensure that tenants enrolled in programs agreed to mandatory random alcohol and drug testing as a condition of participation.

We concluded that the rationale for requiring consent for random drug testing was sound. Impairment resulting from the use of alcohol or drugs could undermine the effectiveness of the programs. Given that cause-effect relationship, we were satisfied that the society's policy provided for the collection of personal information (drug testing constitutes collection of personal information) only for purposes a reasonable person would consider appropriate under the circumstances.

SECTION 12: COLLECTION OF PERSONAL INFORMATION WITHOUT CONSENT

40 Enter Our Free Draw for a Car – and What's the Name of Your Spouse?

When he visited a Victoria coffee shop, an individual noticed a contest to win a new car. He noted that the entrant was asked to provide his or her spouse's name and occupation on the entry form. When our office checked the organization's website, we discovered that individuals could also enter the contest through a website and the online entry form also asked for the spouse's name. An examination of the contest rules and the organization's privacy policy revealed that the contest entries served a dual purpose. In addition to making the entrant eligible for a prize, they were used to collect contact information from prospective clients and obtain their consent for the organization to contact them and present them with various vacation rental offers.

Section 12(1) of PIPA spells out specific circumstances when an organization can collect personal information without consent or from a third party. None of these provisions applies in this particular situation. Under section 6 of PIPA, an organization requires the consent of individuals before collecting their personal information. While consent does not have to be in writing, the design of the contest form was such that it could not be determined if the spouse had consented to the collection of his or her name and occupation and had consented to receiving offers.

Section 7 of PIPA states that an organization must not require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide a product or service. In this case, the entry forms implied that the spousal information was required in order for the contest entry to be valid. However, information about a spouse's name and occupation would not be needed to facilitate entry into a contest draw or to contact the entrant for marketing purposes. In other words, a person wishing to enter the contest and wishing to learn more about vacation property offers does not need to provide someone else's personal information to do so.

Under section 8 of PIPA, an individual is deemed to consent to the collection, use or disclosure of personal information if the individual voluntarily provides it and the purpose of the collection would be obvious to a reasonable person or if the organization makes the purposes known at the time of collection. In this situation, the purpose of the collection for entry into the contest would be obvious (to identify and contact the winner). However, the additional purpose of having the means to contact entrants to pitch products or services is not obvious and must be made known to individuals in order for consent to be valid. The organization's disclosure statement on the back of the paper entry and its online contest rules and privacy policy outlined this purpose for the collection, but lacked clarity.

After we contacted its privacy officer to express our concerns, the organization reviewed its privacy policy and business practices respecting the collection and use of personal information and removed the fields for spousal information from both

the paper and online contest entry ballots. It also rewrote its privacy policy (which was many pages long and packed with legal terminology) to make it concise, easy to understand and compatible with the requirements of PIPA. The organization also modified the official contest rules and the disclosure notice on the paper contest ballots to improve the clarity of the language.

In our complaint investigations, we provide whatever assistance we can to help organizations ensure their business practices comply with PIPA. In this case, the changes resulted in the organization no longer collecting information that was not "necessary to provide the product or service". Persons completing a contest entry form are now provided with clear notice of the organization's intention to contact them to present offers for their products.

Our office does not approve or offer opinions on policy statements of organizations, as we may be called upon later to investigate a complaint abut the policy or actions taken under it if implemented. However, during an investigation or mediation, we will point out areas where an organization may wish to revisit its policies as well as the provisions of PIPA that must be addressed. As was the case in this investigation, cooperation and communication between an organization and our office not only ensures future compliance with PIPA but also helps the organization to avoid complaints from customers concerned about the possible misuse of personal information.

SECTION 13: COLLECTION OF EMPLOYEE PERSONAL INFORMATION

41 Worker Objects to Employer's Insistence on Direct Deposit of Paycheque

A worker on a unionized job objected when his employer notified him that it would no longer pay him by cheque and would require his banking information so that his pay could be deposited into his account. He asked us whether his employer could insist on collecting his banking information for the purpose of paying him by direct deposit.

Section 13(2)(b) of PIPA authorizes the collection of employee personal information without consent if the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.

We concluded that the collection of the employee's banking information was reasonable for the purpose of managing the employment relationship, especially as the collective agreement specified that all employees were to be paid by direct deposit. The employee agreed to provide his banking information.

SECTION 18: DISCLOSURE OF PERSONAL INFORMATION WITHOUT CONSENT

42 Signing Emergency Contact Form Has Unforeseen Consequences

The owner of a strata unit had contracted with a rental management company to lease her apartment to a third party. Later, on receiving a complaint about the tenant, the strata council sent a letter detailing the complaint to the owner, copying the tenant and the rental management company.

The owner complained to us that the strata council had breached her privacy by revealing her name and address to the tenant. She pointed out that the primary reason she had hired a rental management company was to preserve her privacy.

The strata council told us it had obtained the information from the "Notification in Case of Emergency" form, which indicated that the information contained therein was to be used for purposes such as communicating with the owner and tenants and ensuring the proper management of the strata complex. The owner had filled out and signed the form, which provided consent for the strata council to use the personal information to contact the owner, the tenant and the emergency contact. As such, the complaint was not substantiated.

Even though the owner had provided consent, the strata council apologized for any problems the release caused and agreed to amend the form so that the first contact in an emergency would be the rental management company.

43 Co-op Member Shocked by Disclosure of SIN Number

A woman living in co-operative housing got a rude shock when she found a note under her front door with her social insurance number written on it. Her subsequent inquiries led her to believe that a co-op board member had negligently taken members' financial information to her apartment, where it was left out and seen by the person who left the taunting note under her door. She complained to the co-op president, with the result that the board conducted an investigation but was unable to clearly determine what had happened in what amounted to a "he said, she said" situation.

The woman then complained to us that the housing co-op had inappropriately disclosed her personal information. During our investigation, we talked to the president, who assured us that the co-op not only took the matter very seriously but, partly as a result of the complainant's concerns, had taken several measures to safeguard the personal information of co-op members. These included:

- implementation of a key policy requiring all members to sign for keys and obtain a signed acknowledgement upon their return;
- installation of bars and padlocks on filing cabinets in the co-op office and of deadbolts on the office doors;
- blacking out of social insurance numbers on all documentation submitted to the co-op by its members;

- assigning members individual code numbers to use on financial information, replacing names and unit numbers;
- appointing two privacy officers and preparation of a privacy policy to ensure compliance with the *Personal Information Protection Act*;
- shredding outdated documents containing personal information of co-op members; and
- requiring all board members to sign a confidentiality agreement.

The resident argued that her complaint should not be considered resolved until the guilty had been punished with the maximum fine allowable under PIPA. She pointed out that, as a result of the breach, she remained continually fearful that someone might use her personal information to commit identity fraud.

Although we empathized with her distress, we explained that the authority granted to us under PIPA does not include the power to fine those who breach PIPA. Rather, our role is to promote and enforce compliance with the provisions of the legislation – a role which we carry out in large part through public education and the power of persuasion. As we were satisfied that the co-op's board had provided adequate assurance of its determination to ensure compliance with PIPA in future, we closed the file.

44 Condo Owner Livid over NSF Cheque Disclosure

A condo owner was upset with her building's property management company after her cheque for the monthly strata fees bounced when there was a delay in cashing it. Irritation turned to fury when she found out that the property manager had sent a copy of the NSF cheque to the strata corporation together with a detailed statement of her strata fee account from the property management company's automated accounting system.

The woman acknowledged that it was appropriate for the strata corporation to receive information about residents being in arrears, given its responsibility for ensuring payment of fees. However, she strongly believed that, to protect the privacy of condo owners, the property management company should only provide the minimum information needed by the strata corporation. In her view, identifying the resident and the amount in arrears would have been acceptable, but sending a copy of her personal cheque and a detailed statement of her account seemed excessive.

The essence of her complaint to us was that section 18 of PIPA did not permit the property management company to disclose a copy of the returned cheque and the strata fee account report to the strata corporation without the complainant's consent. The property management services the company provided included the processing of payments of strata fees of individual unit owners. Section 12(2) of PIPA permits an organization to collect personal information on behalf of another organization, without the consent of the individual to whom the information relates, if it is needed to carry out work on behalf of the other organization. Section 18(3) permits an organization to disclose

personal information to another organization without consent if it is authorized, under section 12(2), to collect the information on behalf of the other organization.

We concluded that section 18(3) of PIPA authorized the property management company to disclose the strata fee payment information (including copies of cheques) of unit owners of the strata to the strata corporation. The strata corporation, as the governing body of the strata with respect to the household unit owners, represents the organization for the purpose of section 18(3) of PIPA.

SECTION 23: ACCESS TO PERSONAL INFORMATION

45 Former Employee Entitled to Own but Not Others' Personal Information

A former employee of a resort company asked the company for all information regarding his employment. The company replied by releasing some information but withheld information that would identify other individuals.

Section 23 of PIPA obliges an organization to give a person access to his or her personal information subject to a number of exceptions, several of which came into play in this case. Section 23(4)(c) prohibited the company from disclosing personal information about other individuals. Section 23(4)(d) prevented it from disclosing personal information that would reveal the identity of an individual who had provided personal information about another individual and who had not consented to the disclosure of his identity. Finally, section 23(5) required the company to give the former employee his own personal information only if it was able to remove information subject to access exceptions.

Our review of the records in question confirmed that they contained personal information of more than one individual. We also confirmed that the company had given the former employee his own personal information after removing the information to which sections 23(4)(c) and 23(4)(d) applied and, in doing so, had met its PIPA obligations.

46 Fired Employee Not Entitled to Investigation Materials

A care-giver who worked in a seniors' residence got a call from the manager early one morning, as she was preparing to come to work, telling her she was suspended with pay pending the outcome of an investigation. When her employment was later terminated, she protested that she hadn't previously been informed of the allegations of abuse that were provided as the reason for the termination and had been provided no opportunity to defend herself.

A week later she asked the company that ran the residence to release to her any information it had about her that related to the investigation and the reasons for her termination. The company replied that it was withholding this information under section 23(3)(c) of PIPA, which provides that an organization is not required to disclose an individual's personal information to the individual if the information was collected

for the purposes of an investigation and the investigation and associated proceedings and appeals have not been completed.

In this case, the RCMP was still conducting a criminal investigation. Regardless of its outcome, section 23(3)(c) clearly applied, and the company was justified, for the time being, in withholding the information she had requested. We suggested that the applicant consult her lawyer about other possible legal avenues for obtaining the information she felt she needed to defend herself against what she maintained were unfair accusations.

47 Taxpayer Scrambles for Time-sheet Records for CRA Investigation Audit

It's painful enough being investigated by the taxman but even more so when you can't come up with documentation to defend yourself. When Canada Revenue Agency came calling about a man's income tax return, the main issue was his use, as an employee, of a company vehicle and the taxable benefit derived from that use.

When the man asked the company for copies of all his daily time slips he had completed in 2003, he was given instead an electronic spreadsheet that showed the hours worked each day and the days the man had been based out of town at the company camp. The company told him he had already received a copy of each daily time sheet as it was a multi-part form and he had been given a copy at the time of completion. The crunch came when CRA announced that it would not accept the spreadsheet as proof of his time spent in camp, and the company reiterated its refusal to retrieve the original time slips.

When he asked our office to review the company's decision, the man explained that he had lost his copies of the time sheets and that the reason they were important was that he had regularly made narrative comments on the time sheets that described his activities during the day. This additional information had not been collected and recorded on the electronic spreadsheet and was crucial to his case with CRA.

The company told us it had provided all the information the employee had asked for – only the format was different. It added that the time sheets were filed in boxes by particular job rather than by employee name or date, so searching for the man's records would be expensive and time-consuming. The company said it was unlikely that there was much, if any, additional information on the time sheets. We pointed out that the man's comments indicated that there was additional information on the time sheets which would qualify as his personal information and which, accordingly, he was entitled to obtain under section 23 of PIPA. Furthermore, since this was "employee personal information" as defined under PIPA, no fees could be charged for providing the information to the applicant.

The company then located and copied the daily time sheets. As the employee had maintained all along, the time sheets contained handwritten comments describing his day-by-day activities.

48 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 PIPA 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 missing records and the matter was resolved.

SECTION 24: RIGHT TO REQUEST CORRECTION OF PERSONAL INFORMATION

49 The Dental Patient, the Credit Reporting Agency, Two Insurance Companies and Murphy's Law

A woman who applied for a mortgage was shocked to learn that her credit report included a collection notice. The amount owing was in excess of $500 and had been outstanding for over two years. She called the collection company and was told the claim arose from a visit to her dentist.

Further inquiries by the woman revealed a chain of unfortunate events. At the time of the visit, she had been in the process of changing dental insurance companies. As a result, the dentist's office ended up billing her treatment to both of the insurance companies and subsequently received payment from both companies. One payment was applied to the outstanding debt of the patient and the other was retained as a credit on her account. The dentist's office had not notified her of the double payment.

When the patient's previous insurance company realized that it had made a payment for someone who was no longer a policyholder, it sought to recover the money from her. However, she had since married, changed her name and moved to a new address. Unable to contact her, the insurance company turned the debt over to a collection

company, which was also unable to contact her. The outstanding debt was recorded on the woman's credit report.

With this information in hand, the woman contacted the dentist's office. It immediately refunded the money to her and she repaid the amount to the insurance company. She also contacted the collection agency to explain the situation and was assured that the notice would be removed from her credit report. When she received a confirmation letter from the collection agency, it stated that the debt would be noted as paid. A later check of her credit report showed that the notice was still present, but it now indicated the outstanding debt had finally been paid.

After many unsuccessful attempts to have the collection company arrange for the removal of the notice from her credit report, the complainant contacted the credit reporting agency directly to try to have the entry removed. After conducting an investigation, the agency wrote to her explaining that the information on the notice was accurate and factual and no amendment would be made. The letter also advised her that she had the right to add a Consumer Statement (with a recommended maximum length of four lines) to her credit report.

Frustrated, she complained to our office about the refusal of the credit reporting agency to correct her personal information.

Section 24 of PIPA gives individuals the right to request the correction of errors or omissions in the personal information under the control of an organization. If the organization doesn't agree to correct the information, it must annotate (add a note to) the information with the correction that was requested but not made.

In this case, the notice on the complainant's credit report was technically correct. She did have an outstanding indebtedness for a two-year period and it was eventually paid. However, this notice did not accurately reflect the circumstances surrounding the debt.

A basic principle under PIPA is "reasonableness". Section 4(1) states: "In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances". We agreed that it was not reasonable for the complainant to be saddled with the problems which ensued from the placement of the notice on her credit file. The original indebtedness had not resulted from any action on her part and she had been unaware that it had been attributed to her.

When we explained the circumstances to a privacy officer for the credit reporting agency, he agreed the notice should be removed. However, when he then accessed the complainant's credit file, the notice no longer appeared. Someone else at the agency had apparently concurred that it wasn't reasonable for the notice to remain on the complainant's credit file.

Not all situations will result in corrections or removal of offensive material from personal information. It is important to ensure that the organization is made aware of

all the relevant circumstances to assist it in determining whether a correction should be made. Individuals should be aware that if they cannot come to an agreement with an organization over the correction of personal information, they may still have the personal information annotated.

SECTION 28: DUTY TO ASSIST INDIVIDUAL

50 Terminated Worker Challenges Employer's Response to Records Request

Unhappy about having his employment terminated by an organization, a man requested a copy of all his personal information in the organization's custody. In response, the organization provided a package of records with a cover letter explaining the organization was not required by PIPA to disclose information to which solicitor-client privilege applied. When the former employee questioned the absence of emails in the response, the organization conducted a further search for personal information and released copies of some emails responsive to the request.

The man then complained to us that the organization had not conducted an adequate search for records responsive to his request as required by section 28 of PIPA, had not provided an adequate response as required by section 30 of PIPA and had not developed and followed policies and practices necessary to fulfill its PIPA obligations under section 5 of PIPA.

During our mediation of these complaints, the organization conducted another search for records responsive to the applicant's request, including emails. The organization also documented its search efforts and explained its filing system. Based on this information, we concluded that the organization had complied with section 28 by making every reasonable effort to respond as completely as possible.

Section 30 of PIPA requires an organization refusing access to all or part of requested personal information to tell an applicant the reasons for refusal and the provision of PIPA on which the refusal is based. It must also tell the applicant whom to contact in the organization to have questions answered about the refusal and, in addition, inform the applicant of the right to ask the Commissioner to review the organization's decision. In this case the organization's response letter did not provide all this information. During mediation, the organization agreed to provide the applicant with a revised response letter that fulfilled its obligations under section 30. The revised letter resolved this issue.

PIPA requires an organization to develop and follow policies and practices that are necessary for an organization to meet its obligations under PIPA. While an organization is not specifically required to provide a copy of its policies, section 5 does require it to make information about them available upon request. The organization provided us with a copy of its policies and we found it to be in compliance with section 5.

SECTION 32: FEES

51 Patient Seeks Access to Medical Records but Can't Locate Doctor

A man who wanted to obtain a copy of his medical records from his former doctor faced a significant hurdle: the doctor had retired and the man had no idea how to contact him. He wrote to the physician, care of the College of Physicians and Surgeons – the governing body for doctors in British Columbia – which in due course replied that the doctor had kept his records and would provide them for a fee. Section 32(2) of PIPA allows an organization to charge a minimal fee for access to an individual's personal information.

The man then complained to us that the College and the physician were not responding to him within a reasonable time. We contacted the College and the physician and arranged for the physician to provide the applicant with a fee estimate. The physician wanted to use the College as a go-between. The records were copied and provided to the College which, upon receipt of the fee from the complainant, released the records to him.

SECTION 34: PROTECTION OF PERSONAL INFORMATION

52 Company Tightens Security after Personnel File Stolen

A company supervisor drove from head office to meet an employee to conduct a performance evaluation. En route, a bag containing the employee's personnel file was stolen from the supervisor's car.

The company notified the employee, the police and our office. The employee changed his bank accounts and notified the three main Canadian credit reporting agencies, which put a five-year credit watch on his accounts to maintain an alert for any unusual activity. The company agreed to pay for any costs incurred by the employee as a result of the loss of the file.

The company notified all its supervisors and managers of the loss of the personnel file and reminded them of the need to be familiar with the company's privacy policy and procedures. It also decided to provide additional training for staff on protecting personal information and amended its policy on personnel files to require that employee personnel files are no longer to be taken outside the office where they are stored.

After reviewing the company's response to the loss of the personnel file, we were satisfied that it had taken the steps necessary to

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

53 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.

SECTION 35: RETENTION OF PERSONAL INFORMATION

54 Premature Destruction of Investigator's Interview Notes Breaches PIPA

A company hired an independent investigator to examine an employee's complaint that he had been harassed by a co-worker. After the investigator concluded that the charge was unfounded, the employer fired the worker who had made the complaint.

The investigator provided a copy of its investigation report to the terminated employee, who then objected that notes taken during interviews with him were missing and requested all of his personal information from the investigator. When the investi-

gator acknowledged having destroyed the interview notes, the employee complained to our office.

Section 35(1) of PIPA requires an organization to retain an individual's personal information for at least one year if the organization uses that information to make a decision that directly affects the individual, thus ensuring a reasonable opportunity to obtain access to that information.

We concluded that, although the investigator did not terminate the employee and was a separate organization from the employer, it had made a decision that directly affected the employee because the employer had cited the investigator's report as one of the reasons for terminating the employee. For that reason, in order to comply with PIPA, the independent investigator should have kept the notes of its interviews with the employee for at least one year.

4.2 PIPA Order Summaries

55 Order P07-02: 655369 B.C. LTD.

An employee of 655369 B.C. Ltd. complained to us that the organization improperly disclosed her personal information to a co-worker. The information in question concerned the complainant's vacation entitlement.

The Commissioner accepted the complainant's evidence and argument that the only way the co-worker knew the information about her holiday time was by obtaining it from the organization. The organization offered no evidence from the co-worker as to what did or did not occur and could only assert that the only individual who would know the information, the store administrator, denied having disclosed it to anyone other than a union representative.

The Commissioner held that the organization did disclose the complainant's personal information to the co-worker without the complainant's consent. Since there was no suggestion that the co-worker had a job-related need for this information and the disclosure was not for the purposes of establishing, managing or terminating an employment relationship, the Commissioner concluded that the organization had violated section 19 of PIPA and was ordered to stop doing so.

56 Order P07-01: FINNING CANADA

A Finning Canada employee complained that PIPA did not permit his employer to require the production of a driver's abstract by its employees as a condition of employment. An abstract contains information about a driver including height, weight, eye colour and any violations incurred by the driver in the previous five years. The complainant argued that production of a valid BC driver's license was sufficient for the employer's needs.

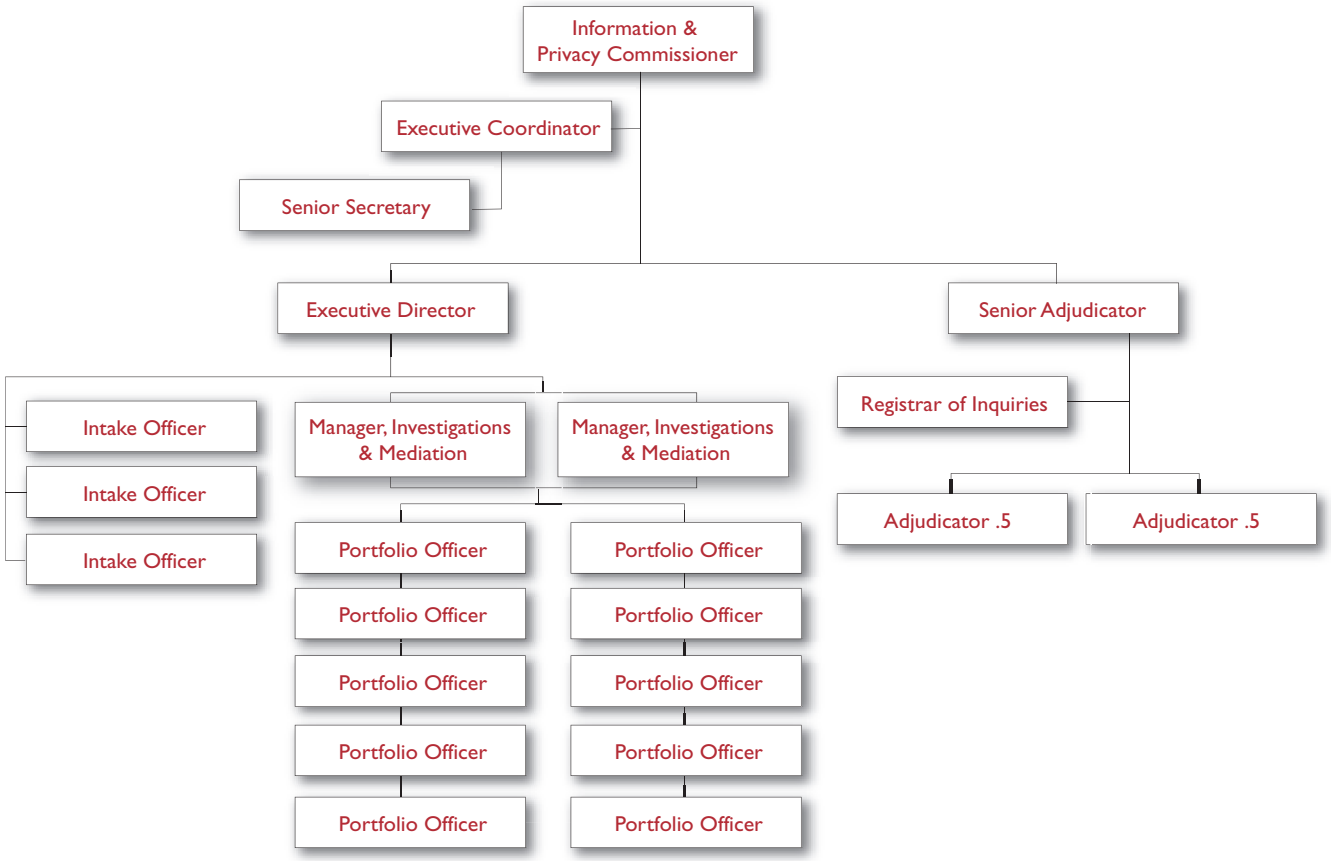
We initially considered the matter to be resolved because Finning decided it did not require the complainant to produce a driver's abstract. However, the complainant

remained concerned about the privacy rights of other Finning employees and asked the Commissioner to rule on his complaint.

The Commissioner reconsidered the matter in order to properly dispose of it under sections 50 and 52 of PIPA and dismissed the complaint because no personal information of the complainant was involved. He also disagreed with the complainant's claim that personal information in the nature of a driving violation history can almost never be reasonably required to establish, manage or terminate an employment relationship, and then only on a case by case basis. For the purposes of section 36(1)(a), the Commissioner said he did not find that Finning's policy presented reasonable grounds to believe that it was not complying with PIPA.

At the time of publication of this annual report, Order P07-01 was subject to an application for judicial review that had not yet been heard.

Organization Chart



Financial Reporting

1. Authority

The Information and Privacy Commissioner is an independent officer of the legislature who monitors and enforces compliance with the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*. The *Freedom of Information and Protection of Privacy Act* applies to more than 2200 public agencies, and accords access to information and protection of privacy rights to citizens. The *Personal Information Protection Act* regulates the collection, use, access disclosure and retention of personal information by more than 300,000 private sector organizations.

In addition, the Commissioner is the Registrar under the *Lobbyist Registration Act*, which requires those lobbying certain public agencies to register and pay a fee.

Funding for the operation of the Office of the Information and Privacy Commissioner ("OIPC") is provided through a vote appropriation (Vote 5), as described below

in note 3, and by recoveries for OIPC-run conferences. All OIPC payments are made from, and funds are deposited in, the Province's Consolidated Revenue Fund.

2. Significant Accounting Policies

These financial statements are prepared in accordance with generally accepted accounting principles in Canada. The significant accounting policies are as follows:

(a) Accrual basis
The financial statements are accounted for on an accrual basis.

(b) Gross basis
Revenue, including recoveries from government agencies, and expenses are recorded on a gross basis.

(c) Revenue
Revenue is recognized when related costs are incurred.

(d) Expense
Expense is recognized when goods and services are acquired or a liability is incurred.

(e) Net Assets
The OIPC's net assets represent the accumulated cost of its capital assets less accumulated amortization.

(f) Statement of Cash Flows
A statement of cash flows has not been prepared as it would provide no additional useful information.

(g) Capital Assets
Capital assets are recorded at cost less accumulated amortization. Amortization is provided on a straight-line basis over the estimated useful life of capital assets as follows:

Computer hardware and software	3 years
Furniture and equipment	5 years

3. Appropriations

Appropriations for the OIPC are approved by the Legislative Assembly of British Columbia and included in the government's budget estimates as voted through the *Supply Act*. The OIPC receives approval to spend funds through separate operating and capital appropriations. Any unused appropriations cannot be used by the OIPC in subsequent fiscal years and are returned to the Consolidated Revenue Fund.

	2008 (UNAUDITED)			2007 (UNAUDITED)
	OPERATING	CAPITAL	TOTAL	TOTAL
Appropriations	$2,952,000	$60,000	**$3,012,000**	**$2,569,000**
Gross Funds Available	$2,952,000	$60,000	**$3,012,000**	**$2,569,000**
Operating Expenses	-$2,929,643	0	**-$2,929,643**	**-$2,314,703**
Capital Acquisitions	0	-$28,329	**-$28,329**	**-$23,000**
Unused Appropriations	**$22,357**	**$31,671**	**$54,028**	**$231,297**

4. Employee Benefits and Leave Liability

Accumulated liability with respect to vacation and other leave entitlements due to employees of the OIPC amounted to $4,562.07 as at March 31, 2008. This liability is fully funded in the Leave Liability Account.

5. Capital Assets

	2007 (UNAUDITED)			2006 (UNAUDITED)
	COST	ACCUMULATED AMORTIZATION	NET BOOK VALUE	ACCUMULATED AMORTIZATION
Computer Hardware and Software	$118,313	-$86,153	$32,160	$20,237
Furniture and Equipment	$11,218	-$5,236	$5,982	$7,510
Total	**$129,531**	**-$91,389**	**$38,142**	**$27,746**

6. Commitments

The OIPC has a leasehold commitment with ARES for building occupancy costs. Payments for office space for the fiscal 2008/09 are estimated at $241,697.00.

7. Pension and Retirement Benefits

The OIPC and its employees contribute to the Public Service Pension Plan ("Plan") in accordance with the *Public Sector Pension Plans Act*. The Plan is a multi-employer defined benefit plan and is available to substantially all of the OIPC's employees. On behalf of employers, the British Columbia Pension Corporation administers the Plan, including paying pension benefits to eligible employees.

The OIPC also contributes, through the Province's payroll system, for specific termination benefits as provided for under collective agreements and conditions of employment for employees excluded from union membership. The cost of these employee future benefits is recognised in the year the contribution is paid.