OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

2008–2009 ANNUAL REPORT

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

2008–2009 ANNUAL REPORT[1]

JULY 2009

Presented to the Speaker of the British Columbia Legislative Assembly pursuant to s. 51 of the *Freedom of Information and Protection of Privacy Act* and s. 44 of the *Personal Information Protection Act*.

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

Design & Production: Alaris Design
Photographs: David Greer

Your Information Rights

FIPPA

The *Freedom of Information and Protection of Privacy Act* guarantees ordinary citizens the right of access to most information (anything recorded in print or electronic form) in the hands of the more than 2,000 public bodies (primarily provincial and local government agencies) covered by FIPPA. Democracy works best when government is fully accountable to the people it serves. Making access to government information a basic right (subject to a few common-sense exceptions described in the Act) provides ordinary people the means to see how and why public servants make the decisions they do and the details of how public money is spent. FIPPA also sets clear rules on how public bodies can collect, use and disclose your personal information (i.e., all information about you).

PIPA

The *Personal Information Protection Act* extends your right as a citizen to proper care of personal information in your dealings with private sector organizations, such as companies and non-governmental organizations, that for whatever reason collect, use or disclose your personal information. This law gives you the right to find out and see what personal information any organization has about you, to be told how it has been used and if and how it has been shared with any other organization, and to ensure any collection, use or disclosure of your personal information complies with PIPA's requirements.

E-health

The new *E-Health (Personal Health Information Access and Protection of Privacy) Act* creates a legislative framework for the protection of personal health information in databases maintained by the Ministry of Health Services and Health Authorities. Personal health information collected, used or disclosed through databases designated by the minister as health information banks may be disclosed only for health-related purposes or where authorized by law. The E-Health Act also ensures privacy protection for the provincial electronic health record system, including the ability of an individual to make or revoke a disclosure directive that would block access to her/his personal health information, the establishment of an arm's length Data Stewardship Committee responsible for making decisions with respect to secondary use such as health research, whistle-blower protection, and a $200,000 penalty for privacy breaches.

Federal Information and Privacy Laws

As provincial laws, FIPPA and PIPA apply only to British Columbia public bodies and organizations. Needless to say, everybody living in British Columbia has regular dealings with federal government agencies (assuming you pay taxes, for example) and national or inter-provincial private sector organizations such as banks and telecommunications companies. To understand your rights when you're dealing with entities based outside B.C., it pays to become familiar with the federal *Access to Information Act* and *Privacy Act* (federal counterparts to FIPPA) and the *Personal Information Protection and Electronic Documents Act* (PIPEDA, federal counterpart to PIPA). The federal counterparts to our office are the Office of the Information Commissioner of Canada[2] and the Office of the Privacy Commissioner of Canada.[3]

2 http://www.infocom.gc.ca/
3 http://www.priv.gc.ca/

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

CONTENTS

REPORT HIGHLIGHTS 1

1 COMMISSIONER'S MESSAGE 5

2 THE YEAR AT A GLANCE: A STATISTICAL OVERVIEW 11

3 INFORMING THE PUBLIC 18

4 RESOLVING PROBLEMS 17

5 ENFORCING THE LAW 52

ORGANIZATION CHART 57

FINANCIAL REPORTING 58

REPORT HIGHLIGHTS

The 5,518 files we closed in our 2008-09 fiscal year (April 1 to March 31) included 905 complaints and requests for review under the *Freedom of Information and Protection of Privacy Act* and 126 under the *Personal Information Protection Act*, an overall increase of 12% over 2007-08. Tables 1 to 8 on pages **11** to **15** provide a thorough statistical snapshot of our activities during the year.

COMMISSIONER'S MESSAGE

Access delayed is access denied. Almost one-third of government responses to information requests under FIPPA exceeded the legislated 30-day time limit and half the responses to political parties were late, on average by three times the time limit permitted by FIPPA. We are glad to see the minister responsible for FIPPA has committed to putting an end to the use of sensitivity ratings and to streamlining government responses to improve timeliness.

E-health legislation needs fine-tuning. The new e-health privacy law is a positive development, but meaningful patient control and other necessary privacy protections are urgently needed.

FIPPA and PIPA are overdue for amendment. It's time the government implemented the amendments to FIPPA an all-party legislative committee recommended five years ago and provided a response on recommended amendments to PIPA.

OIPC response times are improving. We are close to meeting all our performance measures targets, thanks in part to the streamlined "early intervention" process we adopted to ensure a quick resolution and response to straightforward complaints and requests for review.

The wider the sharing of our personal information, the greater the risks. In the name of improved service delivery with reduced costs, the provincial government has initiated a number of new programs that depend on facilitating interagency sharing. Later this year we will report on the safeguards needed to guard against privacy risks of information-sharing. (pp. **5–10**)

INFORMING THE PUBLIC, RESOLVING PROBLEMS, ENFORCEMENT

Our work focuses on the three primary activities mandated by FIPPA and PIPA:

- Informing the public about information and privacy rights and obligations under FIPPA and PIPA;
- resolving the problems brought to our attention (through complaints and requests for review) by mediating solutions consistent with FIPPA and PIPA requirements and acceptable to the disputing parties; and

- when informal resolution proves impossible to achieve, considering any party's request for a formal inquiry resulting in a binding order.

We are fortunate to enjoy a very high rate of success in our mediations – roughly 90% of our files are resolved in this manner. Here are some brief snapshots of some of the mediations summarized in the body of this Report:

FIPPA

POLICE ASSIST REQUESTERS WITH THEIR INQUIRIES

Public bodies have a duty under section 6(1) of FIPPA to "make every reasonable effort to assist applicants…" Requesters can help by being as specific as possible. A woman who had had many encounters with the police over several years complained they hadn't done an adequate search for all her information, as some was missing from the records they sent her. Since she told us she was looking for some very specific information, we suggested she resubmit a narrower request within confined dates. She did, and the police were able to find what she wanted once they knew what she was looking for (Summary 24). At the other extreme, a journalist had a very specific request indeed – that the records he sought from several police departments be provided in Excel format. As the records were very brief, we considered his request reasonable. The departments that had responded with paper copies agreed to enter the information in Excel and provide it to him in that form (Summary 14).

INFORMANTS, COMPLAINANTS AND CONFIDENTIALITY

We helped a WorkSafe BC claimant obtain a summary of information provided by a confidential informant that the claimant assumed resulted in his claim being rejected as fraudulent, though he wasn't told the informant's identity (Summary 12). A ministry employee monitoring work done by a contractor who complained about her had greater success, obtaining the letter written by the contractor and learning as well the identity of the writer (Summary 13).

NO CONSENT FOR RELEASE IF NOBODY THINKS TO ASK

Public bodies denying access to personal or business information frequently don't think to check whether an affected third party (someone other than the applicant and the public body) might consent to the release of information about them. At our suggestion, city officials asked a company if it had any objection to the release of information to which the city had denied access on the assumption it might harm the company's business interests under section 21 of FIPPA; the company having no objection, the information was released pursuant to section 21(3) (Summary 6). And when a man involved in a car accident asked us to intervene after being told by the fire department it wouldn't release the contact information of the other driver or witnesses who had disappeared before the

police arrived on the scene, we suggested that the fire department find out whether or not the other driver or witnesses would consent to the release of that information under section 22(4)(a). While most did not, one did, significantly aiding the cause of an applicant wanting to explore his legal options related to the accident (Summary 4).

COMMUNICATION 101: ASK THE OBVIOUS

Requesters and public bodies sometimes inadvertently neglect to communicate small pieces of information that, if known, would have spared us a complaint or request for review. Such was the case when a public body withheld from an employee two small records because it was unsure who had authored them and hadn't asked. In fact they had been provided by the employee from whom they were being withheld – as was revealed once our investigation got underway (Summary 16). In another case, a man who requested a review of a ministry's decision to release only three recommendations in an investigation report neglected to ask the obvious question, which would have revealed that the report contained only three recommendations (Summary 23).

PIPA

HISTORY DOESN'T CHANGE THE FACTS

Organizations must make a reasonable effort to make sure personal information is accurate if they're likely to disclose it or use it to make a decision affecting the individual. A woman complained that a credit reporting agency refused to remove her bad credit rating even though she had repaid the debt that had caused it. Unfortunately for her, her good efforts didn't change the fact of her previous unpaid debt, and we were unable to substantiate her complaint (Summary 28). In another credit-related file, a car dealership incurred the wrath of a man whose wife was buying a car when it ran a credit check on him without his consent, belatedly explaining it was simply trying facilitate financing eligibility. Following our intervention, the dealership acknowledged the mistake and wrote to the credit reporting agency to have the inquiry deleted from the husband's credit file (Summary 29)

JUST BETWEEN YOU AND ME AND THE GATEPOST – AND PERHAPS YOUR EX-WIFE TOO

The owner of an income tax preparation company got herself in hot water with a client after she disclosed to his former spouse the amount of tax he owed the previous year. Her explanation that he should have told her he didn't want that information disclosed didn't cut it with us – PIPA requires consent for disclosure even to a married partner, let alone to an ex-partner (Summary 30).

AN IDENTITY THIEF'S IDEA OF HEAVEN

The best security systems in the world aren't fail-safe in the face of human error. One organization we dealt with offered a shining example of best practices in securing client personal information with a policy prohibiting retention of personal information on unencrypted storage devices. Then along came some thieves who made off with a portable hard drive. The organization wisely undertook a security assessment to ensure procedures were properly being followed, only to discover that a staff member had backed up several hundred clients' personal information (name, address, phone number, social insurance number, date of birth) in unencrypted form on the portable hard drive. After notifying us of the breach and following our recommended steps for containing it, the organization took the additional precaution of deciding to meet regularly with staff in the future to remind them of their privacy and security obligations (Summary 38).

When a mediation fails, the next step may be a formal inquiry by the Commissioner or an adjudicator. Pages 52–57 summarize some of the orders resulting from inquiries this year.

1 COMMISSIONER'S MESSAGE

You'll notice a number of new things about this year's annual report. Taking a slightly different approach from previous years, we have organized the report into three main sections: Informing the Public; Resolving Problems; and Enforcing the Law. Our goal is to better communicate to the public the main activities and concerns over the past year. Although we have a primary mandate to enforce access-to-information and privacy laws, our less public but equally important role includes settling disputes (and thus avoiding costly enforcement or litigation) and educating public bodies, organizations and citizens about access to information and privacy rights and obligations. Another feature of this report is the emphasis we place on the amount of work we've done over the last year consulting with government and private sector organizations on a variety of policy initiatives.

You'll also notice that this report often gives links to more detailed information on our website. We do this not only because almost everyone will be reading our report electronically – our report has been exclusively electronic for three years – but also because our website serves effectively as a continuing, year-round report on our activities. We use our website on a regular basis as a tool for providing, among other things, updates on our activities; publishing recent orders and investigation reports; offering policy and practice guidance for public bodies and private sector organizations; and posting links to information and privacy news and events nationally and internationally. We try to make our website as accessible as possible and always welcome suggestions for improvement. Earlier this year, we invited public comment on our website and we will be moving ahead with improvements this year.

1.1 Ongoing Delays in Ministry Responses to Access Requests

I expressed concern in last year's message about what I described as a chronic problem at the provincial government level, dating back over a decade, of ongoing failure by ministries to respond overall to requests for access to information in a timely fashion. As I said, access delayed is often effectively access denied and the inability of citizens to exercise their rights to information under the *Freedom of Information and Protection of Privacy Act* in a timely way was cause for grave concern.

Over the last year we have followed through on my plan to begin a program of compliance report cards for ministries, an annual exercise intended to gauge ministry performance against published criteria that measure the timeliness of ministry access responses. In extensive consultation with provincial government ministries, we developed a set of objective criteria and then assessed each ministry's performance against those criteria.

In 2008, almost one-third of the government's responses to access to information requests were late – overdue, on average, by 37 business days – and thus in violation of the law. Of the 22 ministries and other public bodies whose performance we reviewed, only four had an average request processing time of 30 business days or less, 30 business days being the default response time permitted under FIPPA.

Our first report, published in February 2009 for the calendar year 2008, identified serious problems with the provincial government's approach to its access to information obligations under the law. Key findings included the revelation that the government took an average of 35 business days to respond to access requests, managing to respond within the time required by law only 71% of the time, even taking into account permitted time extensions and time during which requests were placed on hold by the public body to allow for consultations with other affected parties. This meant that almost one-third of the government's responses to access to information requests were late – overdue, on average, by 37 business days – and thus in violation of the law. Of the 22 ministries and other public bodies whose performance we reviewed, only four had an average request processing time of 30 business days or fewer, 30 business days being the default response time permitted under FIPPA.

We also were disturbed by the discovery that ministries responded in time to access requests from political parties only 53% of the time, while responding in time to requests from businesses and other public bodies 79% and 94% of the time, respectively. We were also troubled to learn that, when responses to access requests made by political parties were overdue, they were late on average 64 business days, compared to 36 business days late for businesses and 23 business days late for other public bodies.

Given all this, the government's response to our report was very welcome, with the minister then responsible for FIPPA, the Honourable Iain Black, also committing that the government would stop using any kind of sensitivity ratings, as we had recommended. (Sensitivity ratings, which a number of ministries applied until recently were intended to identify information requests considered to be politically sensitive and therefore requiring particularly careful examination.)

More important, the government immediately initiated, and continues to design and implement, an entirely new approach to responding to access requests. A new, centralized approach is being created and streamlining of decision-making processes and new approaches to inter-ministerial consultation are being fashioned. We continue to monitor the situation closely, including through analyzing statistics on request response times, and will continue to offer our expertise to the government as it moves ahead with these much-needed reforms.

As indicated in our February report, we will continue in the future to report, on a fiscal-year basis, on individual ministry timeliness. Regular monitoring will be needed to bring some transparency and accountability to bear on this long-standing problem with provincial government compliance with the legislated obligations under FIPPA. Further, as part of needed ongoing transparency around FPPA compliance, the minister responsible for FIPPA needs to comply with the statutory duty under section 68 of FIPPA to report annually to the Legislative Assembly on government's compliance under the legislation. In the spring of 2009 we received an update for the first quarter of 2009, reporting that

during this period government reduced its processing times from an average of 35 to an average of 27 days and increased the percentage of timely responses from 71% to 79%. This is an encouraging sign that the government intends to follow through on its commitment to improve its processes.

1.2 Electronic Health Information Systems

In last year's message, I noted the passage of the *E-Health (Personal Health Information Access and Protection of Privacy) Act* and acknowledged its significance in filling out the legislated privacy protections for British Columbians in the area of electronic health records. I also noted that key policy choices would have to be made in deciding which of many thousands of health system workers will have access to patient information. I pointed out the need to design privacy into the system through, among other features, robust automated audit controls to capture improper browsing by workers and to give patients a meaningful degree of control over disclosure and use of their personal health information.

I continue to support the e-health privacy legislation. As foreshadowed last year, we have been actively monitoring the development of the provincial e-health system, and have been pushing vigorously for meaningful patient control and for other necessary privacy protections.

I continue to support the e-health privacy legislation. As foreshadowed last year, we have been actively monitoring the development of the provincial e-health system. We have also been pushing vigorously for meaningful patient control and for other necessary privacy protections. I continue to be committed to ongoing consultation with the Ministry of Health Services as it pursues design and construction of the e-health system. In December 2008, I joined the College of Physicians and Surgeons of BC and the BC Medical Association in an approach to the Minister of Health Services, the Honourable George Abbott, urging him and his officials to reinvigorate and expand the process for consultation on critical privacy design issues. The minister's personal commitment to this has been very welcome. We are participating in consultations with the ministry through the Clinical Integration Advisory Committee (CIAC) – as are the BCMA and the College – but we will remain vigilant to ensure that, at the most senior executive levels, the ministry takes the CIAC's recommendations seriously in designing and building the e-health system in compliance with British Columbia's privacy legislation.

1.3 Reforming British Columbia's Access and Privacy Law

It has been more than five years since the last all-party review of FIPPA, yet some of the amendments unanimously recommended by the Legislative Assembly committee that reviewed the law continue to languish. The government has introduced many of the amendments the committee recommended in 2004, but a number of necessary procedural reforms remain outstanding. The government has previously announced its intention of completing those amendments and I again call on the government to demonstrate its commitment to a well-functioning, modern access to information law by completing the amendments.

1.4 Reforming British Columbia's Private Sector Privacy Law

As I mentioned last year, the all-party committee of the Legislative Assembly struck to review the private sector privacy law, the *Personal Information Protection Act*, made a number of thoughtful and sound recommendations to improve PIPA on a number of fronts, without upsetting the balanced and effective policy choices reflected in that law. Over a year has passed since the committee made its unanimous recommendations. The government has, in response to several approaches on my part, said that it will be responding, but without saying when or in what fashion. Although the Committee's recommendations are not significant or controversial, they are necessary in order to improve PIPA. I again call on the government to move with deliberation by introducing amendments to implement those welcome, sound recommendations at the earliest possible opportunity.

1.5 Government Information Disclosures and Delivery of Services – Data Sharing Across Government

In a number of its reports, the Premier's Advisory Council on Technology has called on government to expand the sharing of our personal information in the name of improving service delivery and cutting costs. It is perhaps not surprising that a technology council would be calling for increased sharing of our personal information as a logical means of improving service delivery. While many of us, and I am one of them, agree that modern information technologies may improve service delivery, it is important that demands of efficiency and supposed improvements in service quality not diminish our privacy inappropriately.

The provincial government is moving forward with a number of programs that involve more widespread disclosure, within government and across agency boundaries, of citizens' personal information in the name of improving service delivery and efficiencies. We are actively monitoring and providing comment on these initiatives to ensure that they comply with the existing privacy law and meet reasonable privacy expectations.

I sometimes say the privacy tail should not wag the dog but it is equally important that the technology tail not wag the dog. We have to ask, from a broader policy perspective, whether government's increasing appetite for sharing our personal information creates new and unacceptable privacy risks. The jury is still out on this but important questions have to be tackled. I firmly believe, as do many observers internationally, that information technologies are enabling, and in some senses driving, the creation of more and more personal information databases of increasing scope and sophistication. Our digital selves will increasingly be available, very often on a lifelong basis, as various bits and bytes of ourselves accumulate and grow into a construct that may be distorted and only fleetingly resemble our true selves. As the noted privacy expert Roger Clarke has said, these 'digital personas' may be threatening phenomena given the propensity for governments to use data surveillance to control individual behaviour. We therefore have to be careful to ensure that these digital constructs are not used in new ways, for administrative or other

government purposes unrelated to the original purposes for which the constituent data elements were collected, whether to respond to new policy or legislative directives or in the name of law enforcement.

A pertinent example of data analysis that creates privacy risks involves 'social sorting', which uses personal information to slot individuals, through their digital profiles, into risk or desirability categories. Since inaccuracies in personal information can be broadcast much more widely through data-sharing programs, we can recognize some of the real, concrete risks that are posed for individuals. Proliferation of inaccurate information about an individual could well lead to harmful decisions being made about that person, often without the individual having any way of knowing that this has happened.

Our office is concerned about these trends and as a result we are working on a position paper, to be released this summer, setting out our position on the disclosure of personal information within and across government. Our paper will, we believe, contribute meaningfully to the necessary debate about these issues. It is certainly important that government not move forward with any legislated changes in this area unless and until there has been a full public consultation in the form of a position paper published by the government, followed by meaningful, extensive stakeholder consultations. Something in the order of a White Paper process would be appropriate.

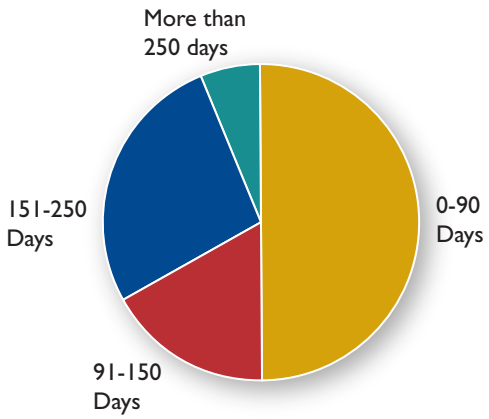
We closed 655 files dealing with requests for review – access to information appeals under both FIPPA and PIPA – during fiscal year 2008-2009 and met, or very nearly met, two of our three targets. We were also either on target or very close to our complaint targets.

1.6 Assessing the OIPC's Performance

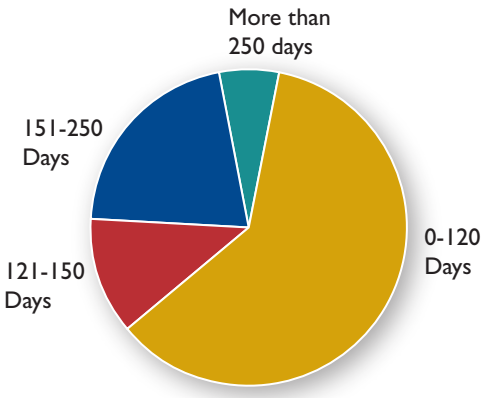
I have publicly indicated several times over the last year that we would start reporting publicly on our own performance in meeting our legislated enforcement obligations. As we discuss in the body of this report, we have measured our own timeliness in meeting legislated response times, in part to improve the quality of our services to citizens but also to identify where further resources might be needed. The following charts show how we've been doing over the last fiscal year. We closed 655 files dealing with requests for review – these are access to information appeals under both FIPPA and PIPA – during fiscal year 2008-2009 and met, or very nearly met, two of our three targets:

HOW OLD WERE THE 655 (FIPPA & PIPA) CLOSED REVIEW FILES DURING 2008-2009 WHEN THEY WERE CLOSED?

	TARGET	ACTUAL
90 business days or fewer	**50%**	325/655 = **50%**
150 business days or fewer	**75%**	438/655 = **67%**
250 business days or fewer	**95%**	615/655 = **94%**



For our complaint files during 2008-2009, we were either on target or very close: We are committed, within the limits of our resources, to doing the best we can to provide services in a timely and effective way. We will work very hard at this as we move down the road.



HOW OLD WERE THE 452 CLOSED (FIPPA & PIPA) COMPLAINT FILES DURING 2008-2009 WHEN THEY WERE CLOSED?

	TARGET	ACTUAL
120 business days or fewer	**60%**	274/452 = **61%**
150 business days or fewer	**75%**	327/452 = **72%**
250 business days or fewer	**95%**	420/452 = **93%**

2 THE YEAR AT A GLANCE: A STATISTICAL OVERVIEW OF OUR ACTIVITIES IN 2008-09

Barbara Haupthoff
INTAKE OFFICER

Tables 1 through 8 below provide a detailed overview of our activities with respect to both the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*. Explanatory notes following each table clarify terms used in the table and the significance of various totals.

Table 1 provides aggregate numbers for all FIPPA and PIPA files combined. Tables 2 through 6 provide a breakdown of statistics for FIPPA files (complaints and requests for review) and Tables 7 and 8 provide a parallel breakdown for PIPA files.

TABLE 1. FIPPA AND PIPA FILES RECEIVED AND CLOSED, 1 APRIL 2008 – 31 MARCH 2009

	DISPOSITION			
FILE TYPE	RECEIVED 08/09	CLOSED 08/09	RECEIVED 07/08	CLOSED 07/08
Information requested/received				
Requests for information	3309	3311	2832	2832
Read and file	91	92	90	88
Media queries	29	27	45	31
Freedom of information requests for OIPC records	9	9	8	5
Requests for review				
Requests for review of decisions to withhold information	630	655	695	575
Applications to disregard requests as frivolous or vexatious	6	4	8	8
Complaints				
Complaints about non-compliance with FIPPA or PIPA	487	452	449	447
Reviews/investigations declined				
Non-jurisdictional	50	50	30	30
No reviewable issue	129	133	99	91
Requests for time extension				
By public bodies/organizations for time extension	277	276	352	352
By applicants for time extension to request a review	34	31	11	12
Reconsideration of decisions				
Internal reconsideration of OIPC decisions	10	7	33	30
Adjudication	2	2	4	0
Files initiated by Public Bodies/Organizations				
Privacy impact assessments	3	4	4	1
Public interest notification	16	17	7	6
Notification of privacy breaches	79	91	92	97

TABLE 1. *continued*

	DISPOSITION			
FILE TYPE	RECEIVED 08/09	CLOSED 08/09	RECEIVED 07/08	CLOSED 07/08
OIPC-initiated files				
Investigations	14	15	11	11
Projects	22	20	21	18
Reviews of proposed legislation	57	60	43	39
Policy or issue consultations	127	114	108	76
Public education/outreach				
Speaking engagements by OIPC staff	74	76	58	55
Conference attendance	24	25	18	21
Meetings with public bodies/organizations	35	28	30	25
Site visit by Commissioner to public bodies/organizations	6	5	1	1
Other	10	14	9	8
Totals	**5530**	**5518**	**5058**	**4859**

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 655 requests for review we completed this year included 621 under FIPPA (Table 2) and 34 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 357 under FIPPA, of which 284 related to access to information and 73 related to protection of privacy (Tables 4 and 5).

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.

Reconsideration of decisions. If a complainant or public body disagrees with the disposition of the complaint, we may reconsider our findings.

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 notify us first.

OIPC-initiated files. Investigation files generally relate to matters with broader privacy or access implications including possible systemic issues. 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.

Other. This category comprises, this year, internal reviews (in which intake officers seek opinions from Portfolio Officers on somewhat complex legal issues such as jurisdictional matters) and teleconferences.

TABLE 2. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY TYPE, 2008-2009

	DISPOSITION								
TYPE	CONSENT ORDER	MEDIATED	NO REVIEWABLE ISSUE	NON JURISDICTIONAL	REFERRED TO PB	WITHDRAWN	OTHER DECISION BY COMMISSIONER	NOTICE OF INQUIRY ISSUED	TOTAL
Deemed Refusal	16	87	0	0	0	1	0	0	**104**
Deny Access	0	68	0	0	0	16	0	8	**92**
Notwithstanding (s. 79)	0	5	0	0	0	0	0	0	**5**
Partial Access	0	291	0	0	0	48	4	34	**377**
Refusal to Confirm or Deny	0	5	0	0	0	0	1	0	**6**
Scope	0	8	0	0	0	12	0	0	**20**
Third Party	0	14	0	0	0	1	0	2	**17**
TOTAL	**16**	**478**	**0**	**0**	**0**	**78**	**5**	**44**	**621**

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. 12-22.1)
Notwithstanding: Conflict between FIPPA and other legislation (s. 79)
Partial access: Some information withheld from applicant (ss. 12-22.1)
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)
Third party: Request for review filed by an individual or business affected by a public body's decision under s. 21 or s. 22 of FIPPA.)

TABLE 3. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY PUBLIC BODY, 2008-09

	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	145	0	0	0	7	0	1	**153**
Ministry of Public Safety & Solicitor General	1	15	0	0	0	7	0	27*	**50**
Vancouver Police Department	0	19	0	0	0	4	0	0	**23**
School District 39	0	19	0	0	0	1	0	2	**22**
Ministry of Attorney General	0	15	0	0	0	3	0	0	**18**
Ministry of Children & Family Development	0	10	0	0	0	6	0	0	**16**
Vancouver Coastal Health Authority	1	5	0	0	0	1	0	6	**13**
Vancouver Island Health Authority	1	7	0	0	0	4	0	0	**12**
Ministry of Health Services	1	7	0	0	0	2	0	0	**10**
Greater Vancouver Regional District	5	4	0	0	0	1	0	0	**10**
City of Vancouver	0	10	0	0	0	0	0	0	**10**
BC Lottery Corporation	1	9	0	0	0	0	0	0	**10**
Top 10 totals	*10*	*265*	*0*	*0*	*0*	*36*	*0*	*36*	***347***
All Other Public Bodies	6	213	0	0	0	42	5	8	**274**
TOTAL	**16**	**478**	**0**	**0**	**0**	**78**	**5**	**44**	**621**

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.

*Twenty-four of the 27 notices of inquiry issued this year to the Ministry of Public Safety and Solicitor General were the result of 24 related access requests made by one applicant.

TABLE 4. DISPOSITION OF FIPPA ACCESS COMPLAINTS, BY TYPE, 2008-09

	DISPOSITION										
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED TO PUBLIC BODY	NO REVIEWABLE ISSUE	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	REPORT ISSUED	TOTAL
Adequate Search	24	18	3	4	26	0	4	0	0	0	**79**
Duty Required by Act	42	24	8	11	32	0	12	2	0	0	**131**
Fees	21	2	0	0	18	0	4	0	1	0	**46**
Time Extension by Public Body	2	21	2	0	1	0	2	0	0	0	**28**
TOTAL	**89**	**65**	**13**	**15**	**77**	**0**	**22**	**2**	**1**	**0**	**284**

TABLE 4 DEFINITIONS:

Adequate search: Failure to conduct adequate search for records (s. 6).
Duty required by Act: Failure to fulfill 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, 2008-09

	DISPOSITION										
TYPE	MEDIATED	SUBSTANTIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	REFERRED TO PUBLIC BODY	NO REVIEWABLE ISSUE	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	REPORT ISSUED	TOTAL
Collection	0	5	1	0	10	0	1	1	0	0	**18**
Correction	0	3	0	0	10	0	0	0	0	0	**13**
Disclosure	6	8	0	2	13	0	1	1	0	0	**31**
Retention	0	3	0	0	3	0	0	0	0	0	**6**
Use	1	2	0	0	1	0	0	0	0	0	**4**
Protection	1	0	0	0	0	0	0	0	0	0	**1**
TOTAL	**8**	**21**	**1**	**1**	**37**	**0**	**2**	**2**	**0**	**0**	**73**

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).
Protection: Failure to implement reasonable security measures (s. 30).

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	DUTY REQUIRED BY ACT	FEES	PROTECTION	RETENTION	TIME EXTENSION PUBLIC BODY	USE	TOTAL
Ministry of Public Safety and Solicitor General	3	0	1	2	13	1	0	0	9	0	**29**
Insurance Corporation of BC	2	1	0	3	6	2	1	0	3	1	**19**
Ministry of Children & Family Dev.	4	0	3	4	3	0	0	0	1	0	**15**
WorkSafeBC	1	3	2	3	4	1	0	1	0	0	**15**
Vancouver Police Dept.	4	1	2	1	4	1	0	1	0	0	**14**
Ministry of Attorney General	3	0	0	2	6	1	0	0	0	0	**12**
Ministry of Health Services	1	1	0	0	7	2	0	0	0	0	**11**
Vancouver Island Health Authority	4	0	1	0	4	0	0	0	1	0	**10**
Ministry of Housing & Social Dev.	3	1	0	1	2	0	0	1	0	0	**8**
Vancouver Coastal Health Authority	1	0	0	0	5	0	0	0	0	1	**7**
City of Vancouver	2	0	0	0	2	2	0	0	0	1	**7**
Ministry of Environment	2	0	0	0	3	1	0	0	1	0	**7**
Ministry of Forests and Range	5	0	0	0	2	0	0	0	0	0	**7**
Ministry of Transportation & Infrastructure	2	0	0	0	2	3	0	0	0	0	**7**
Top 10 totals	**37**	**7**	**9**	**16**	**63**	**14**	**1**	**3**	**15**	**3**	**168**
All Other Public Bodies	42	11	4	15	68	32	0	3	13	1	189
TOTAL	**79**	**18**	**13**	**31**	**131**	**46**	**1**	**6**	**28**	**4**	**357**

TABLE 7. DISPOSITION OF PIPA COMPLAINTS, BY TYPE, 2008-09

	DISPOSITION								
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED TO ORGANIZATION	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	TOTAL FILES CLOSED
Adequate Search	2	2	0	0	0	2	0	0	**6**
Collection	2	1	0	1	3	0	0	0	**7**
Correction	0	1	0	0	5	0	0	0	**6**
Disclosure	5	1	0	3	14	1	0	0	**24**
Duty Required by Act	15	3	3	4	3	5	1	0	**34**
Fees	2	0	0	0	1	0	0	0	**3**
Protection	0	1	0	2	1	1	0	0	**5**
Time Extension by Organization	0	1	1	0	0	0	0	0	**2**
Use	1	1	0	0	3	0	0	0	**5**
TOTAL	**27**	**11**	**4**	**10**	**30**	**9**	**1**	**0**	**92**

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: Failure to implement reasonable security measures (s. 34)
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, 2008-09

	DISPOSITION				
TYPE	MEDIATED	WITHDRAWN	OTHER DECISION	NOTICE OF INQUIRY ISSUED	TOTAL
Deemed Refusal (PIPA)	15	2	0	0	**17**
Deny Access	5	1	1	0	**7**
Partial Access	6	4	0	0	**10**
TOTAL	**26**	**7**	**1**	**0**	**34**

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 INFORMING THE PUBLIC

Mary Carlson
EXECUTIVE DIRECTOR

Both the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act* include in our mandate the duty to keep the public informed about the legislation. We take this responsibility seriously and, in spite of our very heavy caseload, ensure that our schedule includes a wide variety of speaking engagements, presentations at conferences and workshops and participation on panels addressing topical issues. In the current year we co-organized with our Alberta counterparts the 2008 PIPA conference, "Managing Privacy from the Inside Out", which attracted national interest. Our public and annual reports also play an important role in informing the public and we constantly update our website with a view to making it as informative and accessible as possible.

Part of the reason we undertake a wide variety of educational activities is that FIPPA and PIPA each contain many complexities that can cause confusion both for citizens and for the myriad public bodies and private organizations endeavouring to comply with the law. In addition, rapid changes in technology as well as shifting public concerns mean that issues that are highly charged today may take second place to other emerging issues a few years down the road. The risk of identity theft, for example, is a far more pressing concern today than it was when PIPA came into force in 2004.

Part of the reason we undertake a wide variety of educational activities is that FIPPA and PIPA each contain many complexities that can cause confusion both for citizens and for the myriad public bodies and private organizations endeavouring to comply with the law.

We consider it important, therefore, to keep not only the public but also government bodies and private sector organizations well informed about the relevance of information and privacy law to the issues of the day, how to interpret the specific rights and responsibilities prescribed by FIPPA and PIPA, best practices to follow and policies to adopt to ensure compliance with the law, and the need for amendments to keep the laws timely and relevant.

The following is a sampling of some of the events at which we actively participated during 2008-2009:

FIPPA:

- 10th Annual Privacy & Security Conference[4]
- BC Library Association Conference – "What's Up With Government Information?"
- Public Service Agency – Managing in the Public Service Conference
- E-Health Conference – "Health Information Going Walkabout"
- National & International Perspectives on Identity Theft & Fraud – Justice Canada
- New Westminster Police Service – FOI Training for Staff Sergeants and Managers
- BC Association of Police Boards Conference – CCTV Presentation

4 http://www.oipc.bc.ca/publications/speeches_presentations/Reboot(WhereAngelsFeartoTread)(4Feb2009).pdf

Kathie Baker
INTAKE OFFICER

- Vancouver Island University – Presentations to students in Law and Social Services – "Privacy and Information in BC as it Relates to Practice"
- Canadian Bar Association (CBA) FOI and Privacy Law Subsection
- Right to Know Week 2008[5]
- CBA Municipal Law Subsection – "The Growth of Municipal Surveillance"
- CBA National Administrative Law & Labour & Employment Law CLE Conference[6]
- Access & Privacy Investigators' Conference
- Vancouver Island Clinical Research Symposium – "Issues and Implications of Adherence to Privacy Legislation"
- Workshop hosted by BC Civil Liberties – "Radio Frequency Identifiers (RFIDs) and the Future of Humanism"
- Training Seminar for Health Records Site Coordinators – Vancouver Coastal Health Authority

PIPA:

- PIPA 2008 Conference – "Managing Privacy from the Inside Out"[7]
- International Association of Privacy Professionals (IAPP) Canadian Privacy Summit – "The Future of Data Breach Notification and What You Need to Know Now"
- American Bar Association Business Law Meeting – "Canadian Privacy Requirements for US Companies"
- Privacy Compliance (West) Conference
- Canadian Institute Privacy Compliance Conference
- Rotary Club – "Protecting Your Personal Information"
- Workshop for RCMP Volunteers – "Identity Theft and Other Types of Fraud"
- Fraser Valley Real Estate Board – Community Issues Forum
- Condominium Home Owners' Association Vancouver – AGM Symposium
- Educational Workshop for Telus Retirees Group
- Privacy and ID Theft Conference
- Deloitte Security & Privacy Roundtable

Finally, these are a few of the joint projects we embarked upon with our colleagues in other jurisdictions for the purpose of creating educational tools or influencing policies and practices inter-provincially and nationally:

- Memorandum of Understanding between BC OIPC, Privacy Commissioner of Canada ("PCC") and Alberta OIPC with respect to: **Co-operation and Collaboration in Private Sector Privacy Policy, Enforcement, and Public Education**[8]

5 http://www.oipc.bc.ca/RIGHT_TO_kNOW/2008/RIGHT_TO_KNOW_2008.htm.
6 http://www.oipc.bc.ca/publications/speeches_presentations/CBA-CLE_Conf_AdminTribunalsPrivacy(4Nov08).pdf.
7 http://www.verney.ca/pipa2008/agenda.php.
8 http://www.priv.gc.ca/aboutUs/mou_e.cfm.

- Joint Guideline release by BC OIPC, PCC and Alberta OIPC
  Collection of Driver's License numbers under Private Sector Privacy Legislation A Guide for Retailers[9]
- Joint release by BC OIPC and the Ontario OIPC
  Practice Tool for Exercising Discretion - Emergency Disclosure of Personal Information by Universities, Colleges and Other Educational Institutions[10]
- Joint Press Release – BC OIPC, PCC and Alberta OIPC
  Retailers must limit collection of driver's licence information[11]
- Joint Press Release – BC OIPC, PCC and Alberta OIPC
  Privacy Tips for Holiday Shoppers[12]

9 http://www.oipc.bc.ca/pdfs/private/guide_edl_e.pdf.
10 http://www.oipc.bc.ca/pdfs/Policy/ipc-bc-disclosure-edu.pdf.
11 http://www.oipc.bc.ca/news/rlsgen/nr_20081202_edl_e.pdf.
12 http://www.oipc.bc.ca/news/rlsgen/NR-PRIVACY_seasonal_shopping_tips_2008.pdf.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

4 RESOLVING PROBLEMS

Catherine Tully
MANAGER OF INVESTIGATIONS & MEDIATION

Although education and enforcement are significant components of our mandate, the bulk of our office's day-to-day work involves rolling up our sleeves to resolve the problems ordinary people present to us. These problems typically take one of two forms:

- a request for a review of a decision by a public body (under the *Freedom of Information and Protection of Privacy Act*) or an organization (under the *Personal Information Protection Act*) not to release some or all of the information sought by an individual submitting an access to information request; or
- a complaint about a public body's or organization's failure to comply with FIPPA or PIPA by inappropriately collecting, using or disclosing information or by failing to respond appropriately to a request for information.

In 2008-09 we resolved over a thousand request-for-review and complaint files (for a detailed breakdown, see Tables 1 to 8, pp. 11–16). While the number may seem high, it doesn't mean that public bodies and organizations are doing a bad job – quite the contrary. Access to information and protection of privacy are perennially "hot" issues in modern society. The growing number of files we deal with every year simply reflects the keen interest citizens have in exercising their rights both to obtain government information and carefully guard against misuse of information about themselves.

To produce results that are consistently efficient, fair and acceptable to all parties involved, we employ a streamlined approach to mediation, arranging face-to-face meetings if necessary but primarily working by phone. After checking the facts and researching the application of the law to the issues of importance to the applicant or complainant, we may negotiate a resolution with the public body or organization or, if it appears that the public body or organization acted reasonably, explain to the applicant (for a request for review) or complainant why we reached that conclusion. If we believe that a public body or organization has erred but it declines to accept our suggested resolution, we will describe to the applicant or complainant the procedure for requesting a formal inquiry or hearing, by the Commissioner or one of our adjudicators, resulting in a binding order.

Disputes brought to our attention are frequently the result of miscommunication rather than unfair or unlawful treatment. Add to that the fact that information and privacy law is complicated and it's not surprising that confusion frequently accompanies miscommunication.

Mediations of information and privacy disputes require a clear understanding of often complex law. It helps enormously that our office is one of the older legislated information and privacy offices in the world, having recently (quietly) celebrated its fifteenth anniversary. One result of that longevity is that public bodies and private sector organizations, as well as our mediators, can with a few clicks of a mouse access on our website an abundance of orders when there is any doubt about the meaning of a section or subsection of FIPPA. A comprehensive sectional index provides useful direction as to which orders provide the most pertinent and comprehensive analysis.

Like any other organization in the business of resolving grievances, we find that disputes brought to our attention are frequently the result of miscommunication rather than unfair or unlawful treatment. An individual who attempts to achieve something in an interaction with a governmental body or private organization and does not feel heard or feels dismissed or does not receive an explanation in terms he or she can easily understand is an individual who very likely feels aggrieved. Add to that the fact that information and privacy law is complicated and it's not surprising that confusion frequently accompanies miscommunication. The fact that we spend a considerable amount of our mediation time setting the facts and law straight and clearing the air between parties does not mean our time is being misused. Communication difficulties are simply a common reality of human interaction and if we can set matters right without the need for lengthy analysis, then we've done our job.

Another common factor in the grievances brought to our attention is frustration about delays, real or perceived, in responses by public bodies and organizations to individuals' concerns. Simply providing a speedy response, regardless of whether a grievance is found to be substantiated, can be an effective step in resolving it, especially when the grievance itself is rooted in part in frustration about delay or about not feeling heard. That applies as much to our office as to any of the public bodies and organizations we investigate. With that reality in mind we have taken steps to deal with requests for review and complaints in as expeditious a manner as possible, both by implementing performance measures that assess the timeliness of our responses and by developing early intervention procedures to resolve simple complaints and requests for review.

4.1 Performance Measures for Timely Resolutions

FIPPA and PIPA require public bodies and organizations to respond to requests for information within a set number of days. We are also subject to legislated response times with respect to requests for review. That time line is subject to extensions in appropriate circumstances. We are not subject to legislated response times for complaints. However, we decided to establish targets for both file types and periodically measure how well we meet them. Doing so not only enables us to improve our quality of service but also helps us make the most efficient use of our resources in a challenging time.

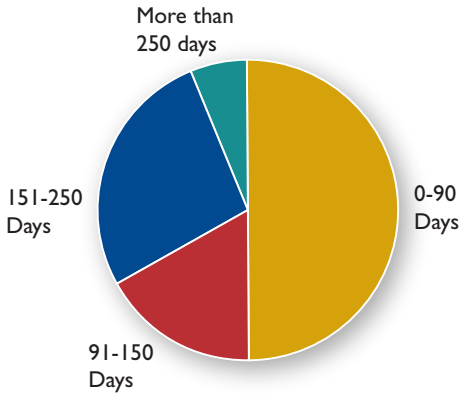
Simply providing a speedy response, regardless of whether a grievance is found to be substantiated, can be an effective step in resolving it, especially when the grievance itself is rooted in part in frustration about delay or about not feeling heard.

After reviewing the performance of other jurisdictions performing similar responsibilities, we decided to set the following targets:

- Requests for review (FIPPA and PIPA): 50% closed within 90 business days of receiving the request, 75% within 150 business days, 95% within 250 business days.
- Complaints: 60% closed within 120 business days of receiving the complaint, 75% closed within 150 business days, 95% closed within 250 business days.

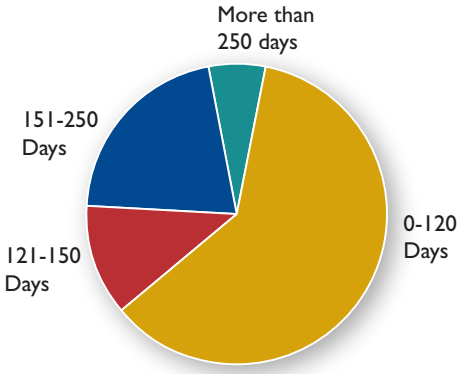
As the pie charts below indicate, we were able this year to either meet or closely approximate the targets we set for closing review and complaint files.

Reviews



Target: 50% within 90 business days
Actual: 50%
Target: 75% within 150 business days
Actual: 67%
Target: 95% within 250 business days
Actual: 94%

Complaints



Target: 60% within 120 business days
Actual: 61%
Target: 75% within 150 business days
Actual: 72%
Target: 95% within 250 business days
Actual: 93%

4.2 Fast-tracking Simple Files through Early Interventions

The Portfolio Officer to whom a mediation or investigation file is later assigned generally takes significantly less time to resolve the matter than was the case prior to our implementation of the Early Intervention Officer process.

One of the mechanisms we have developed for expediting our resolution of straightforward complaint and review files is an early intervention process by which the files are first assigned to an Early Intervention Officer. The EIO's job is to immediately review the file, assess the issue and determine if there is an opportunity for early resolution of the matter. If possible, the EIO will contact the parties to discuss the issues and attempt to mediate a quick solution. If the matter cannot be quickly resolved, the EIO confirms the issues with the parties, obtains the necessary documentation and prepares the file to be transferred to a Portfolio Officer for further investigation or mediation. Experienced Portfolio Officers are assigned to fulfil the duties of Early Intervention Officer on a rotating basis.

The EIO process has been successful in two respects. First, in fiscal 2008 the EIO closed 85 files within an average of 40 business days from our receipt of the request for review or complaint. Secondly, because the EIO has taken the time early on to clarify the issues and prepare the file for mediation or investigation, the Portfolio Officer to whom the file is later assigned generally takes significantly less time to resolve the matter than was the case prior to our implementation of the EIO process.

Although our overall average processing time for a complaint file this year was 104 business days, the average time taken by the Portfolio Officer (i.e., once the file was in the hands of the Portfolio Officer) was only 43 business days. Similarly in the case of reviews, the overall average processing time was 114 business days but, once in the hands of the

Portfolio Officer, a file's processing time averaged only 58 business days. Two years ago, prior to the implementation of the EIO process, Portfolio Officers took more than twice as long to process complaints and took 20 percent longer to process reviews.

Another advantage of the EIO process is that it enables us to limit Portfolio Officer caseloads to a manageable limit of 30 files so that every file receives active and ongoing attention. The EIO files awaiting assignment to a Portfolio Officer also receive active attention from the EIO, who provides an immediate response if anyone calls to inquire about a file or provide new or additional information.

The following brief summaries describe a few of the 85 files resolved this year through our early intervention process.

Cory Martinson
PORTFOLIO OFFICER

Ski Hill Operator Produces Accident Records

A young skier injured himself in a fall from a ski lift while taking lessons. The lawyer hired by his parents to pursue a compensation claim asked the ski hill operation for all records related to their son. When all the lawyer received was a one-page incident report, the parents complained to us that the ski hill had not provided the complete response required by PIPA. Early intervention by our office resulted in the production of further records related to the boy, satisfying the parents that they now had a full response.

No More Massages without SIN

A massage therapist working on contract for a hotel objected to the hotel's insistence that she provide her social insurance number. She believed the hotel didn't need to know her SIN as she paid her own federal deductions. She further claimed that she had brought the issue up with the Canada Revenue Agency, which had supported her position.

Section 12(1)(h) of PIPA provides that an organization may collect personal information if the collection is required by law. We checked the CRA requirement and discovered that employers are required to submit either a contractor's SIN or business number. As the massage therapist did not have a business number, the SIN was required and the hotel could lawfully collect it.

Ministry Questions Identity of Requesters with No Fixed Address

A family facing eviction from their long-time residence on Crown land asked the responsible ministry for any records it had about them. The ministry responded but withheld small portions of the records on the basis that the release of the information would be an unreasonable invasion of a third party's personal privacy.

In our review of the ministry's response, we discovered that the only personal information that was severed was the names of the applicants themselves. The ministry explained that, as the applicants had no fixed address, ministry staff could not be sure they were who they said they were and did not want to release any personal information. By the time our Early

Intervention Officer started working on this file the applicants were represented by counsel and the ministry had agreed to release the records in their entirety to the applicants' lawyer.

Grandfather Asks Hospital for Deceased Son's Records

Believing that negligent care had contributed to the death of his adult son in hospital, a man requested his son's medical records with the intention of pursuing a lawsuit for the benefit of his grandchildren. The hospital denied access on the ground that the requester was not the closest relative or the personal representative of the deceased as required by the FIPPA Regulation. When we initiated our investigation of his complaint against the hospital, we discovered that widow of the deceased man was also named executor in his will and was legally his closest relative as well as his personal representative. As a result, she alone had the right under section 3 of the Regulation to access his personal information in the custody of the hospital.

4.3 FIPPA Mediation Summaries

Individuals who have made an access to information request to a public body and have received a response that withholds information may ask our office to review the public body's decision. We then typically obtain two copies of the records in question from the public body: an exact duplicate of the copy sent to the applicant and an unsevered copy of the requested records. The *Freedom of Information and Protection of Privacy Act* requires public bodies to give reasons for decisions to withhold information. Where information has been severed from a page (i.e., blocked out, either with a felt pen or, more commonly in the case of large public bodies, using a computerized tool designed specifically for that purpose), the public body will typically indicate in the margin of the page the reason for severing simply by referring to the sections of FIPPA (sections 12 through 22.1) that detail the exceptions to the general rule that citizens have a right to obtain copies of information in the custody or control of public bodies. Public bodies that withhold entire documents or sets of records must still explain why.

FIPPA TIP FOR PUBLIC BODIES:

Provide as detailed a reason as possible for each decision to sever information from a record. At the very least, indicate at the precise point on the page where the severing takes place the section AND subsection of FIPPA you are relying upon to sever the information. Also, in your response letter provide a more detailed explanation as to why those sections were applied to particular items of withheld or severed information.

The Portfolio Officer who reviews the public body's decision at the mediation stage (as opposed to the inquiry stage that may take place if the mediation is unsuccessful) then compares the severed records to the "clean" set, considers the reasons provided for severing or withholding information, may refer to previous Commissioner's orders interpreting the section 12 to 22.1 FIPPA exceptions in question, discusses with the public body any concerns about how it has employed the exceptions and, if it appears the public body may have incorrectly applied an exception, may negotiate the release of previously withheld information. If, on the other hand, we concur with the public body's original decision, we will explain to the applicant why we do.

The Portfolio Officer may also discuss with the applicant the right to request a formal inquiry and may candidly discuss as well (with both the applicant and the public body)

the Portfolio Officer's opinion as to what result an inquiry might yield, based on the Portfolio Officer's understanding of previous orders. On this point, it is important to note that, when a matter does proceed to inquiry, the Commissioner or adjudicator has no knowledge of the Portfolio Officer's opinion or any attempts to settle the matter that have taken place during the mediation stage.

As noted in Table 3 (see p.13), our mediations of requests for review involving the Insurance Corporation of British Columbia exceed mediations involving any other public body by roughly tenfold and comprise fully one-quarter of all our mediations. In order to manage this significant portion of our caseload, we decided to assign all our ICBC files to an experienced Portfolio Officer who has developed the expertise and the effective working relationships with ICBC staff needed to efficiently resolve requests for review and complaints related to that public body.

4.3.1 EXCEPTIONS TO THE RIGHT OF ACCESS TO GOVERNMENT INFORMATION

The right of citizens to see information in the hands of government is powerful but not absolute. The exceptions to the rule (e.g., releasing certain information would be an unreasonable invasion of personal privacy, might threaten public safety or would breach solicitor-client privilege) are limited but sometimes complicated. If you're thinking of making an access request but wonder whether some or all of it might fall under one of the exceptions listed in sections 12 to 22.1 of FIPPA, feel free to call us for clarification about how the law works. And if you want to study how the exceptions have been interpreted in the past, click on "orders, investigations and other decisions" on our website, then click on "sectional index" under "public sector".

If the public body you are dealing with decides to sever (withhold) any information from the records you request, it must explain why it is doing so. Typically it will do so simply by marking the relevant section number beside information that has been deleted. For example, if the public body severs some lines of text on the basis that releasing them might be an unreasonable invasion of someone's privacy, all you may see is a whited out area (indicating text has been severed) and "s. 22" in the margin, referring to the FIPPA section that defines the exception. Ideally, public bodies provide a more detailed reason (including referring to the subsection as well as the section), but large public bodies find it difficult to do so because of the high volume of records they process. However, every requester is entitled to ask for and receive a detailed explanation of any decision by a public body to sever records.

The following summaries describe how we dealt with some of the hundreds of requests we received last year for a review of public body decisions not to release requested information.

Disclosure Harmful to Personal Privacy (s. 22)

Summary 1 Public Scrutiny Overrides Job Competition Privacy Considerations

For several years a public body had proactively disclosed to the union with which it had a collective agreement a list of the union members who had competed for each job competition, their seniority and the identity of the winner of the competition. However, in the fall of 2007 the public body decided that for "privacy reasons" it could no longer disclose that information to the union.

Without access to the competition information, the union felt it had no way of ensuring the public body was hiring in accordance with the requirements of the collective agreement. Consequently, the union filed a grievance and made a series of access to information requests. The public body denied access, stating that the disclosure would be an unreasonable invasion of personal privacy within the meaning of section 22 of FIPPA. The union asked us to review that decision.

Section 22(2)(a) of FIPPA provides that, in determining whether disclosure of personal information would be an unreasonable invasion of privacy, a public body must take into account whether "the disclosure is desirable for the purpose of subjecting the activities of the government of British Columbia or a public body to public scrutiny". During the mediation process we initiated in the course of our review, the public body and the union agreed that the disclosure of the limited personal information the public body had released in the past would not be an unreasonable invasion of personal privacy, taking into account section 22(2)(a), as the public interest in ensuring compliance with collective agreements outweighs the privacy interests associated with the type of personal information at issue.

The parties also agreed that the public body was authorized to proactively disclose the information because its disclosure to the union was for a use consistent with the purpose for which it was obtained, as permitted by section 33.2(a) of FIPPA.

Summary 2 Accentuating the Positive Municipality Severs Only Negatives from Audit Report

A newspaper reporter requested a copy of a corporate audit a municipality had conducted on the effectiveness of its administrative operations. The municipality cited section 22 of FIPPA in blacking out the negative comments in the report, including its findings and recommendations. The positive comments were released.

The municipality explained to us that, as the negative comments in the audit report might identify employees of the municipality, it was concerned that releasing those comments might enable identification of those employees and thereby constitute an invasion of their privacy. This explanation was not entirely convincing to us, especially in light of the marked distinction between negative and positive conclusions in the decision whether or not to sever information in the report. Following mediation, the municipality released all of the report except for three very small sections that were subject to section 22(3)(d) of FIPPA.

Summary 3 Reporter Probes for Details on Unprofessional Behaviour Allegations

A member of the press asked a health profession college for copies of reports containing allegations of unprofessional behaviour by college registrants and a description of what had been done to address the allegations.

Although the reporter did not request the names of the parties involved in the incidents, the college concluded that the circumstances described in the allegations were sufficiently sensitive that in some cases simply revealing them might enable identification of the individuals involved. As a result, the college decided to withhold the reports in their entirety, citing section 22(3)(d) of FIPPA, and instead referred the applicant to its web page, which provided a brief description of each disciplinary action and the outcomes. This compromise was of little use to the applicant due to the lack of details supplied in the accounts.

When we began a review of the college's decision to withhold the reports, the college told us that the allegations either had not proceeded past the investigation stage or had been dealt with through the inquiry process – an informal, confidential process by which the parties try to resolve the complaint through some form of remedial action, similar to arbitration. If the inquiry process does not result in a resolution, the college will conduct a hearing – a formal process resulting in a finding of guilt or acquittal. The college was concerned that the small number of such cases in BC – roughly a dozen – meant that disclosure might risk harming the parties' personal privacy. However, in the spirit of openness, the college tried to provide records that would satisfy the applicant's request while protecting the privacy of the registrants and other individuals involved in each case.

The college agreed to supply the remedial agreements or outcomes entered into between the college and the registrants with the exception of personal information that might identify the individuals involved. The applicant was satisfied with this release, but still wanted more detail about the allegations.

The college agreed to release a severed record containing the outline of the allegations and the outcomes. This record provided more detail than the web description, while still protecting personal information belonging to the individuals involved in the incident. The applicant was satisfied with this outcome and agreed to close his request for a review.

Summary 4 Accident Witness Consents to Release of Identity

A fire department received an access request as a result of its quick response to a motor vehicle accident. By the time the police arrived later, some key witnesses and one of the drivers had vanished.

On receiving the other driver's request for the names and personal contact information of all those who had witnessed or been involved in the accident, the fire department withheld that information under section 22(1) of FIPPA. Section 22(1) is a mandatory exception that requires a public body to refuse to disclose personal information where its disclosure would be an unreasonable invasion of a third party's personal privacy.

Caitlin Lemiski
PORTFOLIO OFFICER

Section 22(4) lists categories of information that can be disclosed without causing an unreasonable invasion of third parties' privacy. For example, section 22(4)(a) states that a disclosure of personal information is not an unreasonable invasion of a third party's privacy if the third party has consented to or requested the disclosure. Public bodies do not usually go out of their way to see if consent for disclosure is forthcoming. In this case, we suggested that the fire department take that step. It contacted the third parties and, on obtaining consent from one of them, disclosed his identity and contact information to the applicant. Since the other third parties did not provide their consent, the public body correctly maintained that it was obligated to withhold their personal information.

The public body also took the position that disclosing third parties' personal information would violate section 22(3)(b), which provides that it 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, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation".

While it was not clear to us that the public body in this case had compiled the personal information further to an investigation into a possible violation of law, section 22(1) of FIPPA can apply in the absence of any of the presumed unreasonable invasions of privacy outlined in section 22(3). In our opinion, the public body was required to withhold the remaining personal information.

Satisfied with the additional release of information resulting from our involvement and with our opinion that the remaining information was appropriately withheld, the applicant decided not to request an inquiry.

Disclosure Harmful to the Financial or Economic Interests of a Public Body (s.17)

Summary 5 Liquor Distribution Branch Denies Access to Store Lease Details

In response to a request for records showing the terms of a lease between a shopping mall landlord and a government liquor store, the Liquor Distribution Branch (LDB) provided a copy of the lease but refused to disclose three of its terms, including the lease amount, citing sections 17 and 21 of FIPPA.

Section 17 of FIPPA provides a discretionary exception to the right of access where it can be shown there is a reasonable expectation that disclosing the information would cause harm to the financial or economic interests of a public body or to the government of British Columbia. Section 21 is a mandatory exception that creates a three-part test to determine whether commercial or financial information of or about a third party has been supplied to the public body in confidence and disclosure of the information would cause undue financial loss or gain to any person or organization. Generally, the Commissioner has found that negotiated terms contained in contracts or agreements are not information supplied to public bodies in confidence and section 21 does not apply to this type of information.

We reviewed the information severed from the lease agreement and suggested to the LDB that it did not meet the test of section 21 of FIPPA. In order to determine whether section

17 applied, we then asked the LDB to provide us with evidence that might demonstrate a connection between the disclosure of specific information and the financial harm the LDB had said would likely occur as a result of that disclosure.

The LDB responded with a comprehensive history describing how changes in the licensing regime for retail liquor vendors have brought private liquor retail vendors into direct competition with government liquor stores, not only for customers but also for new and existing retail space. The LDB provided further evidence that, in our opinion, established a connection between disclosure of the information and the financial harm the LDB argued was likely to occur.

During mediation the LDB agreed to release one of the lease terms. After reviewing the withheld information and considering the information provided by the LDB, we concluded there was a reasonable expectation of harm resulting from release of the other two lease terms to the applicant and that section 17 therefore authorized the LDB to withhold this information. The applicant did not agree with this conclusion but chose not to pursue the matter further by requesting an inquiry by the Commissioner.

Summary 6 Patient Reporter Rewarded with City Severance Agreements

A city denied a newspaper reporter access to copies of the severance agreements for two senior employees. The city reasoned that one was not yet finalized and that the release of the other might compromise the negotiation of the yet to be finalized agreement, thereby causing economic harm to the city within the meaning of section 17 of FIPPA.

Before we had an opportunity to draw final conclusions about the validity of the city's position, the city finalized the second severance agreement. The former employee to which it applied consented to its disclosure and the city sent the applicant a copy.

Now that this agreement was concluded, the city notified the other former employee to whom the previously completed agreement applied of its intention to release that agreement, complying with FIPPA's section 23 provision requiring a public body to notify a third party of its intent to give access to a record that the public body believes may contain information that might be excepted from disclosure under section 21 or 22. On receiving the response that he objected to the release, the city told him it had considered his objection and intended to release the agreement despite his objections. The city advised him that he had 20 days to ask us to review that decision in accordance with s. 24(3) of FIPPA. Since he did not do so, the city proceeded to release the agreement, severing only the names and signatures of witnesses.

Disclosure Harmful to Individual or Public Safety (s. 19)

Summary 7 Hospital Information Release to Patient Omits Staff Signature Sheets

A man concerned about the quality of his treatment during a series of hospitalizations asked the hospital for copies of his health records. The hospital withheld only copies of sheets routinely signed by staff to record their signatures to create a running record of staff interactions with patients.

In responding to access requests, hospitals sometimes apply section 19 of FIPPA to sever information the release of which might threaten the safety of medical personnel. In this case, the hospital agreed with us that any risks associated with releasing the sheets of staff names and signatures were non-existent or minimal and agreed to release them in their entirety.

The applicant subsequently realized that he had not received a signature sheet for one of the periods that he was in the hospital. The hospital had not identified the sheet as being withheld as it was missing. When a search failed to locate it, the hospital agreed to recreate the missing record from other sources of the information and give it to the applicant.

Disclosure Harmful to Business Interests of a Third Party (s. 21)

Summary 8 Company Consent Negates City Rationale for Withholding Information

Some "mandatory" exceptions to disclosure in FIPPA, that is, sections 21 and 22, do not apply if an affected third party consents to the disclosure. Too often, in our experience, public bodies fail to consider requesting consent for release of a third party's information before applying the exception they understand to be mandatory.

Upset that his application for a building permit appeared to stall after a city received communications from companies with an interest in the building, a man asked city staff for copies of emails between the city and the companies. The city replied that section 21 of FIPPA obliged it to reject the request because disclosing the emails might harm the companies' business interests. Believing that the emails might have defamed him, the man asked us to review the city's decision.

For section 21 to apply, three requirements must be met:

1. Disclosing the information would reveal trade secrets or commercial, financial, labour relations, scientific or technical information of or about a third party;
2. The information was supplied, implicitly or explicitly, in confidence; and
3. The disclosure could reasonably be expected to result in some kind of third-party harm, such as significant harm to the competitive position of the third party or undue financial loss or gain to any person or organization.

City officials were unable to explain to us how the third part of the test applied to the requested information. We reminded them that, in any event, the prohibition against disclosure does not apply, under section 21(3), if the affected third party consents to the disclosure. As the city had not contacted the companies to explore the possibility of obtaining their consent, we suggested that it do so. The city then obtained the third parties' written consent to disclose the information and the matter was resolved.

Policy Advice or Recommendations (s. 13)

Summary 9 Administrative Emails Are Not Policy Advice

A woman involved in a labour relations dispute with her former employer asked the employer for copies of the records related to the dispute. The former employer provided some

records but denied access to other information, citing the exceptions to the general right of access under sections 13, 14 and 22 of FIPPA.

Dissatisfied with that response, the woman asked our office to review the former employer's decision to withhold certain information. A review of the records led us to conclude that the former employer had appropriately withheld information under sections 14 (legal advice) and 22 (disclosure harmful to personal privacy) but had withheld too much information under section 13.

Section 13 authorizes a public body to deny access to information that would reveal advice or recommendations developed by or for a public body. The intent of section 13 is to allow for the free flow of ideas during decision-making processes, which might be hindered if every suggestion made by or for a public body came under public scrutiny.

Our effort to mediate a resolution included suggesting that the former employer reconsider its use of section 13 and release additional information to the applicant. The employer had applied section 13, for example, to copies of emails that in our opinion were purely administrative in nature and did not contain or reveal substantive advice or other information related to the employer's decision about the applicant.

After the former employer declined to act on our suggestion, the applicant requested a formal inquiry by the Commissioner. However, before an inquiry could be held the applicant reached an agreement with her former employer that resolved her concerns, as a result of which she withdrew her request for review.

FIPPA TIP FOR PUBLIC BODIES

When relying on section 13 to sever advice or recommendations to a public body, be careful to separate out and release purely administrative communications (Summary 9).

Legal Advice (s. 14)

Summary 10 Sidewalk Victim's Lawyer Requests City's Complaint Files

After tripping and hurting herself on a city sidewalk, a woman consulted a lawyer, who advised suing. The lawyer gave a notice of damages to the municipality under section 286 of the *Local Government Act* and six months later asked the municipality for copies of any records it had about complaints made about the sidewalk and repairs made to it. The municipality complied, but withheld four pages under section 14 of FIPPA, which provides discretionary authority for a public body to withhold information subject to solicitor-client privilege. The lawyer asked us to review the decision to withhold the four pages.

The effect of section 14 is to enable a public body to withhold a record that discloses a confidential communication between a lawyer and his or her client that is directly related to providing legal advice. However, for solicitor-client privilege to apply, four conditions must first be met:

1. There must be a communication, whether oral or written;
2. The communication must be of a confidential character;
3. The communication must be between a client (or his or her agent) and a legal advisor; and
4. The communication must be directly related to the seeking, formulating, or giving of legal advice.

Trevor Presley
PORTFOLIO OFFICER

Our review of the records confirmed that all four conditions applied and that the municipality was therefore authorized to withhold them. The municipality consented to our informing the applicant's lawyer that the withheld records were related to an investigation carried out by the municipality's legal advisor for the purpose of providing the municipality with legal advice.

Summary 11 Ministry Misses Mark Describing Solicitor-Client Exception

A man asked for a copy of notes taken in a meeting at which a labour relations issue was discussed. The ministry sent him all but the last paragraph, which it explained consisted of notes from a different unrelated meeting and was therefore outside the scope of the request.

The man subsequently discovered that someone else had requested the same set of notes and that the same paragraph had been withheld, but for a different reason, namely that solicitor-client privilege applied to the final paragraph and therefore the ministry was entitled to withhold it under section 14 of FIPPA. Our review of the paragraph confirmed that the conversation was not between a client and a legal adviser and did not pertain to the communication of legal advice. In short, section 14 bore no relevance to the content.

While the ministry was unable to identify the author of the notes, it seemed clear that this paragraph fell outside the scope of the request. The discussion in it was not consistent with the flow of conversation in the preceding paragraphs and appeared not to be a record of the meeting in question. The applicant accepted our assessment that the original reason for withholding the last paragraph made sense, even though an erroneous reason had been given to another requester.

Disclosure Harmful to Law Enforcement (s.15)

Summary 12 Workers' Compensation Claimant Seeks Identity of Confidential Informant

A WorkSafeBC (formerly Workers' Compensation Board) claimant demanded to know who had provided information about him that, he assumed, led WorkSafeBC to reject his claim as being fraudulent. He asked us to review WorkSafeBC's decision to withhold the informant's identity on the grounds of confidentiality.

We concluded that WorkSafeBC had properly applied sections 15(1)(d), 22(2)(f) and 22(3)(b) of FIPPA. Decisions by public bodies to withhold information about sources of confidential information related to law enforcement are often justified and this was no exception. However, during the mediation WorkSafeBC agreed that it could summarize for the claimant some of the information provided by the confidential source. The claimant agreed to this resolution. Although he would never know the identity of the confidential informant, at least he would know more about the allegations made about him.

FIPPA TIP FOR PUBLIC BODIES

If you decide to withhold information supplied in confidence about a requester, don't forget your obligation under section 22(5) to give the requester a summary of the information unless a summary can't be prepared without identifying the confidential informant (Summary 12).

Summary 13 Complaint Letter about Co-worker Not a Law Enforcement Matter

In the course of carrying out her duty to monitor a ministry's contractors, an employee of the ministry found out that one of them had written a letter of complaint about her to the ministry's regional manager.

Curious about the contents of the letter, she asked the ministry for a copy of it, citing her right of access under FIPPA. The copy of the letter she received in response to her request revealed the identity of the contractor, but some of the opinions the contractor expressed about the applicant had been severed under section 15(2)(b) of FIPPA.

Section 15(2)(b) authorizes a public body to withhold information from an applicant if two tests are met: the withheld information is in a law enforcement record and the disclosure of the information could reasonably be expected to expose to civil liability the person who authored the record or a person quoted or paraphrased in the record. FIPPA defines "law enforcement" as "policing, including criminal intelligence operations; investigations that lead or could lead to a penalty or sanction being imposed; or proceedings that could lead to a penalty or sanction being imposed".

Normally, complaints containing information about tensions or conflict in the workplace are not law enforcement records, under the FIPPA definition. The ministry did not provide evidence to show that the information was part of a law enforcement record and did not indicate how the disclosure of the contractor's opinions could reasonably be expected to expose the third party (the author of the letter) to civil liability.

Because the opinions being withheld were the personal information of both the third party contractor and the applicant, we also considered the application of section 22 of FIPPA. Section 22(1) requires a public body to deny access to personal information if disclosure of that information would be an unreasonable invasion of a third party's personal privacy. In this case, the ministry needed to show that releasing the opinions expressed about the applicant would be an unreasonable invasion of the contractor's personal privacy. The Commissioner's interpretation of section 22(1) in orders published on the OIPC website indicates that only in rare circumstances would the disclosure of an applicant's own personal information to the applicant cause an unreasonable invasion of a third party's personal privacy.

Under section 22(3)(h) of FIPPA, an unreasonable invasion of a third party's personal privacy is presumed to occur if the disclosure could reasonably be expected to reveal that the third party supplied, in confidence, a personal recommendation, or evaluation, character reference or personnel evaluation. The Commissioner has interpreted this type of information to include evaluative information that might be supplied, for example, in a formal performance review or job or academic references. It would not extend to the type of information in the contractor's letter (opinions about a ministry employee's workplace actions or behaviours). Furthermore, even if the contractor's opinions were the type of information contemplated by section 22(3)(h), it is not clear their disclosure would cause an unreasonable invasion of the third party's personal privacy, given the applicant already knew the identity of the third party.

After considering this analysis, the ministry revised its decision and agreed to release the record to the applicant in its entirety.

4.3.2 THE PUBLIC BODY DUTY TO RESPOND COMPLETELY AND PROMPTLY

The drafters of FIPPA took pains to ensure the right of citizen access to government information is truly meaningful by clearly spelling out the responsibilities of a public body once it receives an access request. It's not often you see a law that in so many words requires a government body to "make every reasonable effort to assist" citizens who seek its help, but section 6 of FIPPA says precisely that.

Section 6 also requires a public body to respond without delay openly, accurately and completely. "Completely" means a public body must conduct an adequate search for the requested records regardless of whether they are centrally located or scattered around. FIPPA also requires public bodies to act promptly, delivering the requested records (subject to the exceptions described above) within 30 business days, with time extensions permitted only within narrowly defined circumstances. The summaries below focus on our handling of complaints alleging failure of public bodies to measure up to the standard of duty required by FIPPA.

Summary 14 Reporter Requests Electronic Records, Gets Paper Response

FIPPA TIP FOR PUBLIC BODIES

Provide the record in the format requested, even if it requires extra work to do so, if it will not unreasonably interfere with your operations (Summary 14).

A newspaper reporter sent identical requests to eight municipal police departments asking for records relating to police salaries. In each case, he asked that the responsive records be provided in Microsoft Excel so he could include them in a searchable database he was constructing. Five of the police departments sent him the records in Excel as requested; the other three provided paper copies, without explanation. The reporter complained to us that the three police departments had not responded appropriately to his request.

Section 6(1) of FIPPA requires a public body to make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely, while 6(2) requires it to create a record for an applicant if doing so "would not unreasonably interfere with the operations of the public body". We explained to the three police departments that in previous orders the Commissioner had found, for example, that requiring a public body to hire a programmer for 48 hours to respond to an applicant's request to produce records did not unreasonably interfere with the operations of the public body. It seemed very likely that responding to the reporter's request for an Excel response would take a small fraction of that effort.

The result of our mediation was that all three police departments agreed to provide the reporter the records in electronic form. As the requested records did not exceed two to three pages, it was easy to enter them in Excel if they were not already in this format. The reporter was happy with the resolution.

Summary 15 Previous Viewing of Records Does not Preclude Later Right of Access

A man who asked a government ministry for certain records within a specific date range later complained that the ministry had not responded accurately and completely and had not provided sufficient reasons for refusing access to some of the requested records.

Section 6(1) of FIPPA obliges a public body to make every reasonable effort to assist applicants and to respond openly, accurately and completely. In its initial response, the public body took the position that it did not need to provide all the records within the specified date range because the individual had previously viewed some of those records. After we pointed out that nothing in FIPPA precludes an individual from asking for a copy of a previously viewed record, the ministry agreed to release all the records within the specified date range.

FIPPA TIP FOR PUBLIC BODIES

The section 6(1) duty to assist applicants and to respond openly requires public bodies to make a special effort to help out requesters (rather than, say, taking every opportunity to shut the door).

That might mean, for example, making records available even if a requester has already seen them (Summary 15). Responding "openly" also means communicating as fully as possible with the requester and working diligently to address and resolve any concerns raised by the requester.

Summary 16 Incomplete Release Package Triggers Suspicion of Incomplete Search

A public body employee, dissatisfied with his employer's investigation of an incident involving himself and another employee, requested access to records related to the incident.

On receiving a response, the employee noticed that a few records were missing and complained to us that the public body had failed to provide the complete response required by FIPPA. The Commissioner has concluded that the section 6(1) requirement to respond "completely" means public bodies are expected to conduct a search for records that a fair and rational person would consider appropriate in the circumstances. FIPPA does not impose a standard of perfection.

The complainant told us that proof of an incomplete search lay in the fact that three records were obviously missing from the package provided to him. The missing records included his original complaint letter to the public body, a letter written on behalf of the applicant and a transcript he had prepared of a conversation with another employee. Our review of the records revealed that the public body had included the complaint letter in the release package and had withheld the other two records because it was unsure who had authored them. Once the public body was able to confirm that the two withheld documents had been provided by the complainant, it agreed to release them to him. He was satisfied with this outcome.

FIPPA TIP FOR PUBLIC BODIES

When in doubt about the origin of records, make sure they were not supplied by the requester before withholding or severing them (Summary 16).

Summary 17 Ministry Goes Extra Mile to Assure Requester of Adequate Search

A man who asked a ministry for information related to public-private partnerships complained to us that there must be substantially more records responsive to his request than the relatively small number the public body provided to him. He felt certain this was the case given the significant issue of public spending related to the subject matter of his request.

On its own initiative, the ministry suggested that if the applicant wished to speak with a well-informed employee of the public body it would arrange for him to do so. The

applicant agreed and an appointment was set up. After the meeting, the applicant told us he was satisfied as a result of his meeting with the employee and now believed he had received all responsive records.

Summary 18 College Extends Response Time Limit to Consult with Registrants

A patient asked a regulatory college for records concerning a complaint he had made about a college registrant. When the college failed to respond within the 30 business-day deadline set by section 7 of FIPPA and extended the time limit, the patient complained to us about what he considered an unjustified time extension.

Section 7(2)(a) of FIPPA provides that a public body is not required to respond within 30 business days if the response time limit is extended under section 10. Section 10(1) authorizes public bodies to extend the time limit for responding for up to 30 business days if (a) the applicant did not give enough details for the public body to identify the requested records, (b) a large number of records were requested and meeting the time limit would unreasonably interfere with the public body's operations and/or (c) more time is needed to consult with a third party or another public body before deciding whether to release information. Section 10(2) also authorizes public bodies to extend the time limit for periods greater than 30 business days with the permission of the Commissioner.

The college told us it had extended the time limit by 30 business days because it needed to consult with the registrants involved in the complaint before deciding whether to release the records to the applicant. After confirming that the college had in fact consulted the two registrants, we were satisfied that it had appropriately relied upon section 10(1)(c) to extend the time limit.

Summary 19 Health Authority Denies Having Custody of Care Facility Records

FIPPA specifically provides, in section 3, that it applies to all records in the custody of or under the control of a public body. What sounds, in theory, like something that would be easy to determine is often much more elusive in practice.

Faced with a request for various records of a long-term care facility managed by a non-profit society, a health authority responded that the records were in the custody and control of the long-term care facility, not the health authority, and were therefore subject to the *Personal Information Protection Act* rather than FIPPA. The applicant complained to us.

We began our investigation by looking for factors that would indicate whether the health authority or the non-profit society had custody and/or control of the records, which consisted of contracts, board meeting minutes of the non-profit society and other documents.

One factor that suggested that the records were subject to PIPA was the management of the facility by a non-profit organization was a legal entity distinct from the health authority. On the other hand, the non-profit provided contracted services on behalf of the health authority and in this case had entered into a contractual arrangement whereby the health authority had the power to direct the non-profit society in regard to asset transfer

FIPPA TIP FOR REQUESTERS

If your request is sufficiently complicated to generate a significant fee estimate and you believe there's a public interest argument to be made under section 75(5) for a fee waiver, make sure you fully understand the circumstances under which a waiver in the public interest is likely to be supported. See, for example, Order No. 332-1999 on our website.

and the transfer of "ongoing obligations." In addition, several executives of the health authority sat on the board of the non-profit society.

We advised the non-profit and the health authority of our initial conclusion that the requested records were likely subject to FIPPA. After considering our comments, the health authority and the non-profit agreed to provide the applicant with the requested records rather than requesting an inquiry.

Summary 20 Municipality Replaces Inaccurate Fee Estimate with Full Waiver

The drafters of FIPPA wanted to preclude the possibility exorbitant fees being used as a *de facto* way of blocking access requests. They recognized as well that provision should be made for reasonable fees both to reflect the time and expense of responding to access requests and to guard against abuses of the right of access. FIPPA describes a middle ground that seems to work well for the most part.

Section 75 of FIPPA says that a public body cannot charge for the first three hours spent locating and retrieving a record or for the time spent severing information from a record, but can charge a reasonable amount for time spent locating and retrieving a record, in excess of three hours, and for basic costs of production and shipping. Section 7 of the FIPPA Regulation spells out specific costs for specific tasks – e.g., 25 cents per copy for photocopying records.

Public bodies that deal with a large number of access requests are usually quite familiar with the fee structure FIPPA permits. Understandably, many small public bodies are not. The fee disputes we're called upon to resolve are divided more or less equally between disputes about the amount of the fee estimate and rejected applications for fee waivers in the public interest.

In one such case, an organization that promotes the interests of architects asked a municipality for copies of records and drawings related to a recently approved resort development project. When the municipality estimated a cost of $1,000 to compile and copy the records, the organization requested a fee waiver, arguing that the municipality should exercise its discretion under section 75(5)(b) to waive the fee as the requested records related to a matter of public safety insofar as they had to do with building design and safety. The municipality denied the fee waiver request and the organization complained to us that the denial was unreasonable.

Our review of the municipality's fee calculations revealed several errors. The municipality had

- charged 50 cents a page to photocopy the records, doubling the maximum allowed by section 7 of the FIPPA Regulation,
- charged $50 per copy of a plan drawing when the maximum allowable is $1 a square metre,
- estimated $300 dollars for staff wages without providing a breakdown,
- included GST in the fee estimate and
- charged for the first three hours of search time, contrary to the FIPPA requirement not to do so.

When we pointed out its errors, the municipality decided to waive the fee in its entirety.

Summary 21 Frustrated Researcher Finally Strikes Pay-dirt on Public Body Website

FIPPA TIP FOR REQUESTERS

To get the best bang for your buck, always first consider alternative sources of information to making a request (Summary 21) and carefully word your request so it as clear and narrow as possible (Summary 24). The more precise your request, the less likely it is that the response will be delayed or the public body will miss finding what you're really looking for.

By narrowing requests for information to the bare essentials, individuals can often save themselves and public bodies a great deal of time and effort and obtain a desired result without frustrating delay.

A researcher asked a large public body for records describing its financial assets. The public body provided a fee estimate of several thousand dollars for the production of the requested information and dismissed the researcher's contention that the fee should be waived because his research served the public interest.

During mediation, the researcher told us he would be satisfied simply to learn the methods by which the public body calculated certain financial information, without knowing the actual dollar amounts. The public body showed how to access this formula on its website, thus resolving the complaint.

Summary 22 Clarification Confirms Completeness of Building Project Records

A developer asked us to review a municipality's response to his request for records relating to a building project in which he had an interest. He told us the records did not contain all the information he expected would be relevant to his request.

We reviewed the records and found little severing. When the developer clarified the type of information he thought was missing, we confirmed that the records already contained what he was looking for. What was required was a more detailed reading than he had initially undertaken. The municipality communicated directly with the developer in order to further clarify the contents of the records.

The developer said he would consider the matter resolved if he received two pieces of information: a complete copy of a building permit and a confirmation of a certain cost calculation. The copy of the permit provided to him did not include the information that would usually be set out on this form. The municipality explained that the permit had been created, in exceptional circumstances, after the project was completed and therefore did not contain the usual information. We reminded the applicant that correspondence earlier released to him explained that this had taken place.

With regard to the cost calculation, the separate figures provided in the records did not tally exactly with the final total. The municipality checked for more records without success. The applicant was satisfied on this point when the municipality confirmed the nature of the separate costs and clarified that the records indicated that the final calculation had been provided by an employee of the applicant.

Summary 23 Recommendations Brief, Action Plan Lengthy, Records Complete

A man who asked a ministry for records relating to an investigation of a workplace conflict was pleased that, as a result of our review of the ministry's response to him, more records were released.

His only outstanding concern was about a ministry employee's comprehensive analysis based on recommendations in an investigator's report. The applicant wanted the complete set of recommendations as those that were disclosed did not appear to support the far-reaching analysis.

After discussion with the ministry, which confirmed that it had released the complete investigator's report, we explained to the applicant that the apparent discrepancy between the three brief recommendations and the lengthy analysis was due to the fact that the analysis was intended to be a comprehensive action plan incorporating a perceived need for more changes. Brief as the recommendations may have been, they were substantial enough to trigger a very detailed implementation strategy.

Summary 24 Narrowed Request Helps Police Locate Additional Information

Individuals requesting their personal information from public bodies or private organizations with which they have had many dealings increase their chances of obtaining effective results by being as clear as possible about what it is they are looking for and, whenever possible, providing dates and similar markers that can help the organization to expedite the process by narrowing the search.

A woman who asked a police department for all of the information it had about her complained to us that the department hadn't done a thorough enough search, as some information was missing from the records sent to her. Section 6 of FIPPA sets out the duty of a public body to assist applicants and states that:

> 6(1) The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.

Since it was not clear from the wording of the complaint what information the complainant believed to be missing, we asked her to provide some clarification. She did so by providing relevant dates of certain encounters she had had with the police over the years. This clarification (in effect, a narrowed request) enabled the police department to locate some additional records and provide the applicant with a new response about them.

Although some information had not been uncovered in the department's earlier search, we concluded that it had complied with section 6 of FIPPA. The standard required in searching for records is not one of perfection, but rather that a public body must do that which a fair and rational person would expect to be done or consider acceptable. The search was considered reasonable in this case for two reasons: the police department gave us a reasonable explanation for not searching two particular areas the first time; and it was not clear from the applicant's request that she was looking for a particular type of record.

FIPPA TIP FOR REQUESTERS

Always thoroughly check the records you receive from a public body before jumping to the conclusion that something has been left out. You'll save yourself a little embarrassment and save our office and the public body the time it takes to deal with a request for a review of the public body's decision (Summary 22). And if you still believe something may be missing, make your concerns known to the public body before seeking our help – sometimes there's a very simple explanation of why the records are or are not complete (Summary 23).

4.3.3 FIPPA COMPLAINTS

Pat Egan
PORTFOLIO OFFICER

Collection of Personal Information by Public Bodies

Summary 25 Law Enforcement Purpose Justifies Collection without Notification

A woman complained that a regulatory agency – a public body under FIPPA – had contacted third parties without her knowledge as part of an investigation it was conducting about her. The agency confirmed to us that it had indeed contacted third parties and collected personal information about the woman without her knowledge or consent.

Section 26 of FIPPA permits a public body to collect personal information if a specific provision in a law authorizes the collection. In this case, the regulatory body's enabling statute contained specific provisions giving the regulatory body the power to collect personal information about individuals without their consent in certain circumstances, which we determined applied in this case.

Furthermore, under section 27(3) of FIPPA, the public body was exempted from the standard obligation to notify the individual whose information was collected because it was investigating a law enforcement matter. The definition of "law enforcement" in FIPPA includes "investigations that lead or could lead to a penalty or sanction being imposed." In this case, the public body's enabling legislation permitted it to issue a broad range of penalties and sanctions. Consequently, we were unable to substantiate the woman's complaint.

4.4 PIPA Mediation Summaries

The majority of the conflicts brought to our attention under the *Freedom of Information and Protection of Privacy Act* have to do with requests for access to information rather than the collection, use and disclosure of personal information. Not surprisingly, the reverse is true for the *Personal Information Protection Act* – most people who seek our help have a conflict with an organization about how their personal information has been collected, used or disclosed. Another key difference in our approach to resolving PIPA problems is the need for a greater emphasis on educating organizations about their obligations to protect clients' and others' personal information, and providing advice to organizations on how to meet those obligations in a practical and cost-effective manner.

Now that the legislation is five years old, large organizations are generally up to speed on PIPA requirements, but thousands of smaller organizations may have had little occasion to worry about privacy until the day a letter of complaint turns up in our inbox. The media blitz on the perils of identity theft in recent years has been a large factor in heightening consumer awareness of privacy issues. The average consumer nowadays may not only have installed a shredder beside the printer but may also be in the habit of questioning the collection of their personal information by businesses ("You'll only let me buy a widget if you can record my driver's licence number? That's against the law!") and demanding to know how businesses intend to use and disclose the information they do collect.

To help organizations familiarize themselves with their PIPA obligations, we have developed plain-language guidelines that we post on our website and update from time to time.[13]

Collection of Personal Information by Organizations

Summary 26 Electronic Key Fob Tracks Condo Residents' Entries

A condo unit owner complained that residents' key fobs were designed to be electronically read every time the building was entered. The result was that the key fob information could reasonably identify an individual in circumstances where there was only one resident occupying the unit associated with that fob. The building had instituted the key fobs (similar to electronic cards used by hotel guests) because it was cheaper than re-keying the whole building.

Because section 2(2) of the *Strata Property Act* provides that a strata corporation has the power and capacity of a natural person with full capacity, strata corporations are organizations subject to the requirements of PIPA. Our general preference in dealing with PIPA complaints is to work with organizations to resolve complaints cooperatively whenever possible, rather than simply determining whether or not a complaint is substantiated. If we find that an organization's practices violate PIPA requirements, we may also help the organization explore ways to bring its practices into compliance with PIPA.

Section 12(1)(h) permits an organization to collect personal information without consent if the collection is required or authorized by law. The practice complained of did not meet this requirement. However, as a result of the complaint, the strata corporation subsequently passed a bylaw authorizing the collection of key fob data. Under the *Interpretation Act*, a bylaw has the same weight as any other enactment.

Even if the collection is authorized by law, section 11 of PIPA requires that the information be collected only for the purposes that a reasonable person would consider appropriate in the circumstances. To ensure that requirement was met, the strata corporation also created a policy that set reasonable limits on the collection, use, disclosure and retention of personal information collected from key fobs. For example, the policy requires the strata corporation to destroy the information after a set period of time and says that key fob data may only be accessed to investigate instances of serious property damage.

While the complainant would have preferred not to have electronic key fobs at all, she was glad that the strata corporation's new policy reduced the risks associated with their use.

PIPA TIP FOR CITIZENS

Organizations generally cannot record a customer's personal information unless they clearly need to do so in order to be able to provide their services. A store may ask to see your driver's licence to verify your identity but cannot insist on photocopying the licence or writing down the number (Summary 27). Sometimes, allowing a business to record your driver's licence information can lead to unexpected and unwelcome consequences (Summary 29).

Summary 27 Store Can View Driver's Licence but Cannot Insist on Recording Its Information

A customer of a large grocery store complained about its practice of requiring shoppers who made purchases of more than $250 to produce a driver's licence and then recording the personal information from the licence. The store argued its practice was necessary to guard against identity fraud and consequent financial losses for the store.

13 http://www.oipc.bc.ca/pdfs/private/a-_GUIDE_TO_PIPA(3rd_ed).pdf.

We considered whether the store sought to collect personal information beyond what was necessary to provide a product or service, which would have violated section 7(2) of PIPA, and whether it was collecting information that a reasonable person would consider to be appropriate in the circumstances, as required by section 11(a) of PIPA.

We concluded that, while viewing a person's driver's licence may be necessary to prevent purchases being made with false identities, the information contained on the licence need not be written down for an organization to sell its products. A reasonable person would not object to a cashier viewing a driver's licence to verify a person's identity, but would object to the information on the driver's license being recorded because that information need not be recorded to complete the sales transaction while preventing identity fraud. This conclusion is consistent with the Commissioner's findings in Order P05-01, posted on our website at http://www.oipc.bc.ca/PIPAOrders/2005/OrderP05-01.pdf.

Consequently, we concluded that the actions of the store's employees contravened sections 7(2) and 11(a) of PIPA and that the complaint was substantiated. The grocery store agreed to cease writing down driver's licence information and to destroy any records containing such information.

Accuracy of Collected Information

Summary 28 Debt Repayment Doesn't Erase Bad Credit History

However well you learn from your past mistakes, once you've made them they're part and parcel of your personal information. And nowhere are past financial slip-ups more glaringly obvious than in a person's credit history.

A customer's default in a loan repayment resulted in a bad credit rating. After making a cash settlement with the lending company, she asked the credit reporting agency to remove the bad rating as the matter had been resolved, then complained to us that the credit agency had refused her request.

Section 33 of PIPA requires an organization to make a reasonable effort to ensure that personal information it collects is accurate and complete if it is likely either to use the information to make a decision affecting the individual or to disclose the information to another organization. In addition, section 24 requires it to correct personal information on being satisfied on reasonable grounds that a request for correction should be implemented.

We concluded that the credit agency was not required to correct the bad rating, even though it would almost certainly disclose it to another organization the next time the woman applied for credit. The fact that the woman was more than 120 days late on her payments meant she had earned the bad rating. Settling the matter with her creditor did not change the fact that the posted information was accurate, so there was no reason to alter the credit history.

Use of Personal Information

Summary 29 Auto Dealership's Helpful Credit Check Backfires with Customer's Husband

When a woman took a car for a test drive, the dealership's salesman took a copy of her husband's driving licence as well as her own in the expectation that each of them might take a turn at the wheel, even though they had made it clear she alone was doing the buying. The woman ultimately decided to purchase the vehicle and filled out an application for financing.

The following week, on checking with a credit reporting company, the husband noted that the dealership had just checked his credit status. (Credit reporting companies are required by section 23 of PIPA to report to requesting individuals the sources of their credit information.) He complained to us that the dealership had improperly used his personal information without his consent, as his wife was buying the car and it had nothing to do with him.

The dealership explained to us that it was merely trying to be helpful. When it became obvious that the woman would not be eligible for financing, the dealership did a credit check on the husband, hoping that this information might help complete the transaction. The dealership acknowledged that it did not have the complainant's authority to conduct a credit check and was aware he wasn't a party to the purchase.

As section 6 of PIPA provides that an organization must not use personal information about an individual without consent, we found the complaint to be substantiated, as it was clear that section 15, which permits use without consent, had no application here.

Acknowledging its error, the dealership wrote to the credit reporting agency and asked it to remove the record of the business's inquiry from its records. The credit reporting agency confirmed to the complainant that it had deleted the inquiry from his credit file. We also gave the dealership suggestions for resources that would help it meet its section 5 obligation to develop the policies and practices needed to ensure compliance with PIPA.

PIPA TIP FOR ORGANIZATIONS

Disclose customers' personal information without their consent only in the very limited circumstances allowed by PIPA. It is against the letter and spirit of PIPA to adopt a practice of "opt-out consent" – requiring customers to notify you if they do NOT want their personal information disclosed (Summary 30).

Disclosure of Personal Information

Summary 30 Long Arm of Privacy Law Extends Even to Confidentiality between Spouses

A man complained that the organization that prepared his income tax return had disclosed his personal financial information, namely the amount of tax he owed from a previous return, to his former spouse. When he objected, the organization told him he should have given them a letter stating he didn't want such information disclosed.

When we called the organization, the owner readily acknowledged that the disclosure had taken place and was inappropriate. She explained she had been preparing the tax returns for the complainant and his spouse for years and that during the latest tax year her clients had separated but continued to live together at the same residence and use the same phone. Assuming her clients were still sharing financial information, the owner had disclosed the information in the course of preparing the tax returns of the complainant and his former spouse.

Darrel Woods
PORTFOLIO OFFICER

Although the business owner's assumption about the nature of her clients' relationship was understandable, the disclosure was not authorized by PIPA – and would not have been even if the clients had not been separated. We suggested that, in future, she always obtain the consent of couples before sharing their personal information, regardless of whether they are spouses or separated. We suggested that developing a consent form that could be signed and filed in the relevant tax return file each year would be a good way to formalize the process. The owner agreed to implement this recommendation and later provided our office with a copy of the form she had developed.

Informed of the results of the investigation and the resolution we had reached, the complainant said he considered the matter adequately resolved.

Summary 31 Temp Worker Accuses Former Employer of Disclosing Her Employee Information

A temporary employment agency contracted a woman's services to a third-party organization. While working there, the woman noticed several workplace deficiencies that she brought to the organization's attention. When no action was taken to remedy the problems, she complained to the public body that regulates the third-party organization.

After the public body initiated an investigation into her allegations, the organization attempted to find out who had complained about its deficiencies. Suspecting the temporary worker had made the complaint, the organization made several calls to the employment agency in an effort to obtain her personal information. Assuming that the temporary employment agency had responded by giving out her employee personal information, the worker complained to us about the inappropriate disclosure.

Employee information includes information such as home phone number, home address and identity numbers. Under PIPA, personal information includes employee information and the same protections apply.

Our investigation revealed several potential sources from which the organization might have acquired the complainant's personal information. The temporary employment agency denied wrongly disclosing her employee information and we found no evidence it had done so. We concluded that the complaint was not substantiated.

PIPA TIP FOR ORGANIZATIONS

If a customer asks you for copies of her or his personal information, you must (subject to very limited PIPA exceptions) provide it all – not just contact information and descriptive data but also such items as records of interactions with the customer and opinions about the customer (Summaries 32 ,33 and 35).

Access to Personal Information

Summary 32 Patient Requests Access to Description of Her Dispute with Doctor's Office

Miscommunication between a patient and doctor's office staff about appointment scheduling led to a heated argument and a decision by the patient to change doctors. Staff prepared a statement of what had taken place so management would be well informed if they needed to deal with the matter further and informed the patient that they were doing so.

The patient asked the doctor's office to send copies of all her professional records to her new doctor's office and to send a copy of the statement to her directly. When she didn't

receive it, she sought our assistance, explaining that it was important to her to know what the statement contained as she feared the term "statement" meant that the organization might make a formal complaint about her to some higher authority.

The organization told us that although it had sent out a copy of the client's professional records as requested, it had not sent her a copy of the statement as it was not part of the professional record. After obtaining and reviewing a copy of the statement, we explained to the organization that section 23 of PIPA requires an organization to provide to an individual who requests it "the individual's personal information under the control of the organization".

Acknowledging that the statement consisted largely of personal information about the applicant, the organization agreed to give her a copy after severing some personal information of third parties.

Summary 33 Tracking Missing Pieces of Employee File

A man who lost his job at a store asked for a copy of his "file". The employer, a large retail chain with a regional headquarters in Vancouver and a head office in Washington state, produced a copy of his personnel file from the store where he had worked. He complained to us that the organization had not conducted an adequate search for the information he had requested because his personnel file did not contain information about health benefits and WorkSafeBC claims he had made while working at the store.

Upon receiving a written access request, and subject to certain exceptions, an organization is required by PIPA to give an individual his or her personal information under its control. It must make a reasonable effort to assist each applicant and to respond to the access request as accurately and completely as reasonably possible. Part of the organization's duty to respond completely includes making a reasonable search for information responsive to the access request. FIPPA prescribes a similar duty, which the Commissioner has interpreted to mean that a search must be conducted that a reasonable person would consider satisfactory under the circumstances. This duty does not require perfection.

We contacted both the local Human Resources Services Manager and the Director of BC stores and were told the organization had understood the complainant's request to be for his personnel file, which does not normally contain claim information. Explaining that the organization was unlikely to have any significant claim information, as employees usually make claims directly to the insurer, they suggested that access requests could be made directly to the insurers and provided the contact information for both insurers as well as for the organization's Benefit and Claims Manager in Washington state. We suggested that the complainant pursue these avenues, noting that while he certainly had a right to make a request to the organization's Washington state office, it was less certain that our office had the authority to investigate its response.

An additional issue arose when our investigation revealed that the organization had withheld some information from the personnel file without informing the complainant. PIPA requires organizations to inform individuals when their personal information is being

withheld and to explain why. The organization agreed with us that there was no need to withhold this information and subsequently released it to the complainant. As the complainant did not subsequently respond to our phone calls or letters, we were unable to determine whether he was satisfied with our resolution of his complaint.

Summary 34 Company Correctly Releases Only Personal Information of PIPA Requester

Citizens who are generally aware of their access to information rights may not be familiar with the significant differences in the access rights PIPA and FIPPA. While FIPPA provides a right of access (with specified exceptions) to all types of information, PIPA provides a right of access only to the personal information of the person making a request.

In response to a man's access request, a company withheld some information on a number of grounds, including that it was not the individual's personal information as defined in PIPA or was personal information about another individual. The requester, who was not aware of the narrow limits of his right of access under PIPA, asked us to review the company's decision to withhold information.

Our review of the records revealed that the withheld information included work product information as well as information about the organization, its employees, its agents and other third parties. Such information is specifically excluded from PIPA's definition of personal information. Further, under section 23(4)(c) of PIPA, an organization must not disclose personal information about another individual. We concluded that the company was authorized and/or required to withhold the information it did.

Our explanation of PIPA and its application to an individual's own personal information satisfied the applicant and we closed the file.

PIPA TIP FOR ORGANIZATIONS

No matter how small your organization or what the nature of its activities, if someone asks you in writing for her/his personal information in your possession, you have an obligation under PIPA to find what you have and provide it to the requester (subject to PIPA's limited exceptions) within 30 business days (Summary 36).

Summary 35 Coach Seeks Copy of Letter about His Coaching

When a minor league coach found out someone had sent a letter to the governing association concerning his coaching practices, he asked the association for a copy of the letter and was refused access.

Section 23(1) of PIPA requires an organization to provide an individual with the individual's personal information (defined by PIPA as information about an identifiable individual) in the custody of the organization. In certain circumstances, however, an organization is required to *not* release an individual's personal information. Two of the mandatory exceptions described by section 23(4) applied to this case. Under section 23(4)(c) an organization must not disclose personal information when the disclosure would reveal personal information of other individuals. Under section 23(4)(d) an organization must not disclose personal information when disclosure would reveal the identity of the person who provided the personal information about the other individual (in this case the applicant) and the individual who provided the information does not consent to the disclosure of her or his identity.

We read the letter in its unsevered form and confirmed that it contained the personal information of the coach as well as other individuals. Because the coach claimed to know who wrote the letter, the association was reluctant to release any part of the letter, fearing that doing so would reveal or confirm the identity of the letter writer. When we told the coach that PIPA entitled him to receive his own personal information but not the personal information of others or information that would reveal the identity of the letter writer, he indicated that if his personal information was disclosed to him he would consider the review resolved.

In an effort to mediate a resolution, we suggested the association approach the letter writer about consenting to the release of a version of the letter severing everything but the applicant's personal information. The letter writer consented to have the letter released in this form. When the applicant received a copy of the severed letter he considered the matter resolved.

Summary 36 Unaware of PIPA Obligations, Social Club Ignores Access Request

Four years have passed since PIPA became law but many organizations, though they may appreciate the importance of personal privacy in general terms, remain unaware of their own obligations under PIPA, which defines the organizations to which it applies to include persons, unincorporated associations, trade unions, trusts and not-for-profit associations.

A member of a social club had a falling-out with the organization and asked for a copy of all his personal information in its possession. After receiving no acknowledgment of his request, he complained to us about the club's failure to respond.

Section 28 of PIPA requires organizations to make a reasonable effort to assist applicants and to respond "as accurately and completely as reasonably possible." Section 29 requires that response to be made within 30 business days of receiving the request for information.

The social club had never heard of PIPA. However, after we explained the legal obligation to respond, the club wrote to the applicant and responded to his request for his personal information.

Summary 37 Job Applicant, Employment Agency Dispute Access to Reference Interviews

A woman applied for a job advertised by an employment agency hired by a company to pre-screen potential employees. The prospective employer was expecting to receive a short-list of candidates, with at least two references, transcripts of conversations by agency staff with the person's references, the candidate's test results if relevant and a summary of his or her initial interview with the agency.

The agency asked the woman to sign a disclosure statement and release form before proceeding to deal with her application. She objected to the fact that the form prevented her from receiving the confidential transcript of any conversations between the agency and any of her potential references. She refused to sign the form and complained to us that the agency had violated section 7 of PIPA by insisting she sign the form as a precondition to receiving the agency's services.

PIPA TIP FOR CITIZENS

If you apply for a job and consent to references being contacted, you can subsequently ask to see the information provided by the references – but in responding to you, the employer must sever any information about you the release of which would reveal the referee's identity unless the referee has specifically consented to his or her identity being disclosed to you (Summary 37).

Justin Hodkinson
PORTFOLIO OFFICER

In order to comply with section 7, the employment agency had to show that its collection, use and/or disclosure of the applicant's personal information were necessary to provide the employment agencies services. The release form's purpose was to seek an applicant's consent to authorize the agency to contact anyone associated with any entry on a person's résumé in order to obtain references. We concluded that such a broad authorization contained in the form, if signed, was neither "necessary" nor "indispensable" because the agency only required two references, one of which had to be the applicant's direct supervisor. We suggested the agency amend its form to ask each applicant to provide a list of potential references, including at least two direct supervisors. The agency was then to contact only those potential references listed.

The applicant also argued she should be entitled to the transcripts of the agency's interviews with her references. The agency maintained that, as references' information was provided in confidence, it could not be shared with the applicant unless the person granting the reference consented. Subsections 23(4)(c) and (d) of PIPA stipulate that the agency must not reveal the identity of a third party. This means that unless the reference consents to his or her identity being disclosed, it will be severed from any transcript of any interview. In practice, the referee will decide if the information was provided in confidence or not. If even a summary of the transcript would allow an applicant to surmise who supplied the reference, then the applicant would receive neither the content of the reference nor a summary of it. The agency agreed to cease obtaining references "in confidence" and to amend its release form.

4.5 Public and Private Sector Privacy Breaches

Public bodies and private sector organizations need to be particularly diligent in developing and maintaining security systems to guard against inadvertent breaches of privacy that may involve large numbers of people or sensitive personal information. The obligation to maintain adequate security extends not only to physical safeguards but also to ensuring that staff keep well informed about internal policies and practices for guarding against information breaches. We strongly recommend that public bodies and private sector organizations alike familiarize themselves with our recommended steps for dealing with privacy breaches, posted on our website.[14]

Summary 38 High Calibre Security System Undone by Human Error

A private sector organization contacted us to report a privacy breach resulting from the theft from its office of a portable hard drive containing the sensitive personal information of its clients. The information was not encrypted, allowing the thieves to view the clients' personal information. Thieves commonly use this type of personal information to commit identity theft.

Section 34 of PIPA stipulates that a private sector organization must make reasonable security arrangements to protect personal information in its custody or under its control.

14 http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches(June2008).pdf.

The four key steps an organization should take to manage a privacy breach include containing the breach, evaluating the risks, determining whether notification is required and developing prevention strategies.

On discovering the theft, the organization notified the police, who attended and conducted an investigation. The organization's Privacy Officer was alerted to the theft on the next business day. The organization conducted a security assessment to determine if the office had complied with security policy, to guarantee security procedures were now being followed and to reinforce the importance of following security protocols. They discovered that a staff member had backed up personal information onto the portable hard drive without encrypting the information, contrary to the organization's security policy. The employee was immediately disciplined for the breach of policy.

Although the office had excellent building security systems in place, the thieves managed to exploit a vulnerability. The organization repaired the damage, thus securing the premises from a repetition of the theft. We concluded that the organization had taken appropriate steps to contain the breach.

In order to determine what additional steps are immediately necessary, organizations are expected to evaluate the risks associated with the breach. In this case, the theft included several hundred clients' personal information, consisting of name, address, phone number, social insurance number and date of birth. In this case, the organization's assessment of the potential harms determined that the clients were vulnerable to identity theft and fraud.

Immediate notification to affected clients is important to mitigate any harm that may have occurred. The organization mailed letters to its clients notifying them of the date of the breach, together with the nature of the breach and the type of information stolen, describing the steps already taken to mitigate the harm and the short and long term strategies to prevent future breaches, and advising the clients of steps they could take to reduce the risk of harm. The letter also provided the contact information for both the organization's Privacy Officer and our office.

Staff followed up the letter by calling all of their clients, reviewing the types of information lost and precautionary measures taken, and offering to pay for clients' credit monitoring services.

Our only concern about the notification process was the delay from the time the breach was discovered to the time the clients were notified. Organizations should make every effort to notify clients as quickly as possible so precautionary measures are implemented immediately.

The "reasonable security arrangements" section 34 of PIPA requires include meeting industry standards that require the encryption of portable storage devices containing sensitive personal information. The organization's existing policies prohibited retention of personal information on unencrypted storage devices. The breach in this case resulted from human error.

We concluded that the organization had good security policies and systems in place to protect personal information. It has now added the additional precaution of meeting regularly with staff to remind them of their privacy and security obligations.

PIPA TIP FOR ORGANIZATIONS

The best security practices in the world for the protection of clients' personal information can be defeated instantly and massively by human error. Regularly remind staff of your privacy protection procedures – and if a privacy breach does occur, promptly follow the steps listed on our website for containing it and preventing another in the future (Summaries 38 to 40).

Summary 39 Missing Computer Server Compromises Hotel Guests' Privacy

The very night that a hotel's ownership was to change hands, the hotel's server, containing information about hotel bookings, went missing. The new owners called the police and then, understanding that a privacy breach had occurred, contacted us as well.

Our investigation revealed that, under the previous ownership, the server room had not been alarmed and access had not been logged. The server had not been bolted to the floor or otherwise affixed to the room and the door had frequently been left open in order to ventilate the server room.

Section 34 of PIPA requires an organization to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. When a breach occurs, an organization should (in accordance with the guidelines posted on our website) contain the breach, evaluate the risks, determine whether notification is required and develop prevention strategies.

In this case, the new owners were limited in how they could contain the breach, because the server was never found. After the new owners contacted the police and alerted staff that the server was missing, they anticipated the risk of identity theft and decided to notify affected individuals by letter. They also installed an adequate ventilation system and made plans to install a swipe-card access system that logged entry. In short, the new owners took adequate steps to remedy the breach and prevent its recurrence in the future.

Summary 40 Personal Information Disappears after Courier Pick-up

Documents containing personal information of a number of individuals went missing and appeared to have been lost in transit between a service provider and a public body. Although a courier had picked up the documents, there was no record of their receipt.

Under section 30 of FIPPA, public bodies in British Columbia must protect the personal information in their custody or under their control. There are four key steps for managing a privacy breach: every reasonable effort to recover the personal information must be made; steps should be taken to minimize the harm resulting from the breach; affected individuals must be notified; and the public body must take steps to prevent future breaches from occurring.

While we found the public body's response to the breach to be in compliance with section 30 requirements, the case illustrated the need for both public bodies and private organizations to put in place special safeguards for courier transport of personal information. These safeguards are summarized in our office's publication, "Physicians & Security of Personal Information", prepared following breaches involving medical information[15]:

14 www.oipc.bc.ca/pdfs/private/PhysicianSecurityofpersonalinformation.pdf.

TRANSPORTING RECORDS BY COURIER

Choose a courier company that has implemented the security safeguards listed below. It is vital that they demonstrate that they consistently practice these safeguards.

Safeguards to Consider

- Ask the courier company what security measures it employs to protect personal information. Some measures that should be employed are:
    - Physical security in their offices and areas where the personal information is stored, including locked storage, alarms and monitoring;
    - Restricting employee access to personal information;
    - Ensuring drivers are bonded and insured;
    - Having staff sign confidentiality agreements;
    - Driver guidelines and policy that ensure the personal information is kept secure while in the vehicle; and
    - A method to track the shipment of records that requires the receiver's signature.
- Ensure the courier company tracks the shipment and collects the signature of the receiver when the delivery is made.
- The sender should record an itemized description of the documents being transported in case there is a discrepancy about what documents were received, or in case any missing files need to be identified.
- When transporting records containing personal information by courier, consider calling the receiver to confirm pick up and ask it to confirm receipt of the records.

Summary 41 Privacy Breach Backfires, Mayor Loses Election

A village resident complained that the mayor had handed out her personal information at a chamber of commerce meeting. To check the facts, we called the village administrator, who confirmed that, at a meeting the administrator chaired, the mayor had disclosed personal information of the complainant he had obtained from the village records. This disclosure was contrary to section 30.4 of FIPPA, which prohibits public body employees from disclosing personal information obtained in the line of work unless authorized to do so by FIPPA. The mayor had sought to use the information to prove a point that would embarrass the complainant.

Following the mayor's disclosure and before we received the complaint, the village administrator emailed staff and council and also held a training session reminding them of their obligation not to disclose personal information they come across in their work. We suggested as well that the new councillors elected in the upcoming election receive training on freedom of information and privacy issues and the administrator agreed to ensure this took place. The complainant ran against the mayor in the election, won the mayoralty and then declined to pursue her complaint with us any further.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

5 ENFORCING THE LAW

Celia Francis
SENIOR ADJUDICATOR

As a dispute-resolving body, our office is unusual in that we combine the practice of mediation with the authority to issue legally binding orders. We can negotiate a solution that all parties are happy with or we can order one particular party to do or stop doing something so that it complies with FIPPA or PIPA. By contrast, the Office of the Ombudsman, established 15 years before our office came into being, must rely solely on its power to persuade.

Our combination of mediation and order-making authority provides a practical range of alternative tools that complement one another. Parties appreciate the opportunity for mediation because it's free, informal and quicker than an inquiry, but if they cannot agree on a satisfactory outcome, the applicant can also ask for an inquiry leading to a binding order, without ever leaving our office.

If our best efforts to mediate a resolution to a dispute under FIPPA or PIPA fail to yield a result the parties can agree upon, then we discuss with them the option of proceeding to an inquiry. If the applicant requests an inquiry and the request is granted, then the Portfolio Officer who mediated the dispute draws up a statement of the facts and issues that resulted in the matter being brought to our office. In all other respects, the person conducting the inquiry (the Commissioner or a delegated adjudicator) has no knowledge of anything that transpired during the mediation phase. The parties to the dispute are then invited to make submissions to the inquiry and potentially affected third parties may be invited to do so as well.

The written order comprehensively analyzes the facts, issues and application of the law and provides the rationale for the legally binding order. All orders are posted on our website immediately after they are issued.

5.1 Orders and Decisions

The following summaries represent a selection of orders and decisions made by the Commissioner and adjudicators during the 2008-09 fiscal year.

Order F08-08 – College of Psychologists of British Columbia

Parents involved in a custody and access dispute hired a psychologist to prepare a "psychological assessment" of them and their daughter. The mother requested access to a citation related to another individual's complaint that the college had issued against the psychologist, and the college decided to disclose it in severed form. The psychologist requested a review of this decision, saying the entire record should be withheld. The adjudicator found that the relevant circumstances favoured disclosure and ordered the college to give the mother access to the severed citation.

Decision F08-07 – Ministry of Labour and Citizens' Services

The applicant requested a copy of the "Workplace Support Services" contract between IBM Canada Ltd. and the Ministry of Labour and Citizens' Services. After seeking comments from IBM, the ministry decided to disclose some of the information and IBM requested a review of that decision. As mediation of the request for review did not resolve the matter, an inquiry was scheduled. The ministry and IBM raised a number of objections to the issues as set out in the notice of inquiry, as a result of which the Information and Privacy Commissioner considered first whether the original applicant had standing to participate in the inquiry and whether the ministry was required to release part of the requested records to the applicant regardless of IBM's request for third-party review.

The Commissioner rejected the ministry's and IBM's arguments that IBM's request for review froze the ministry's duty to respond to the applicant's access request on other exceptions. He directed the ministry to provide the applicant with its response to the applicant's request. He also concluded that the applicant was an "appropriate person" to participate in the inquiry regarding the section 21 issue. This decision was the subject of a judicial review not yet heard at the time we prepared this annual report.

Our combination of mediation and order-making authority provides a practical range of alternative tools that complement one another. Parties appreciate the opportunity for mediation because it's free, informal and quicker than an inquiry, but if they cannot agree on a satisfactory outcome, the applicant can also ask for an inquiry leading to a binding order.

Order P08-02 – Bowman Employment Services Inc.

The applicant requested access to her personal information in Bowman's file concerning employment services it provided to her. The organization provided a fee estimate of $535 based on the applicant's original request for her complete file and, later, another fee estimate of $753 for what the applicant considered to be a narrower request. The applicant complained the fees were not reasonable and should be reduced or excused. The adjudicator confirmed that the first fee estimate was "minimal". She found that the second fee estimate was not "minimal" and ordered it reduced to $51.

Order F08-22 – Fraser Health Authority

A union representing employees of Sodexho MS Canada Limited requested access to "renewed or newly signed contracts, including amendments, appendices and schedules" between the Fraser Health Authority and Sodexho for housekeeping services in the FHA hospitals. FHA decided to disclose the records with some information severed under section 17(1) (harm to the public body's financial or economic interests) of FIPPA and section 21 (harm to third-party business interests). The union requested a review of that decision and, as mediation did not resolve the issues, the matter proceeded to inquiry.

The Commissioner found that FHA was not authorized by section 17(1) or required by section 21(1) to refuse to disclose the pricing terms in an addendum and change order to a multi-year contract for housekeeping services in hospitals. He ordered FHA to provide access to the disputed information. This decision was the subject of a judicial review not yet heard at the time of the writing of this annual report.

Michael McEvoy
ADJUDICATOR

Order F08-13 – Ministry of Public Safety and Solicitor General

A woman requested video footage taken of her while she was held in custody at the Vancouver City Jail. The ministry refused access on the basis that disclosure would compromise the jail's security system, thus endangering the life or safety of staff, correctional officers, individuals in custody and visitors. In addition, the ministry argued that section 22 of FIPPA required it to withhold information relating to other individuals in custody but not that relating to officers working at the jail. However, the third-party officers, whose images were on the videos, objected to the disclosure.

The adjudicator concluded that there was no persuasive evidence that releasing the videos, which revealed incidents of interest to the applicant, would endanger the life or physical safety of a law enforcement officer or harm the security system of the jail. The ministry was required to provide access to some of the video footage but was ordered to withhold other information that identified other individuals held in custody. The fact that the videos would identify the third parties in their employment capacity did not render disclosure of the videos an unreasonable invasion of privacy. This order was the subject of a judicial review not yet heard at the time of the writing of this annual report.

Order F08-20 – Vancouver Police Board

The Vancouver Police Board refused a request from a journalist for a copy of a "target silhouette and inscription" that the Chief Constable of the Vancouver Police Department gave to the City of Vancouver Manager. The Board argued that disclosure would be an unreasonable invasion of the Chief Constable's personal privacy because it related directly to his employment, occupation or educational history. The journalist argued that the Chief Constable had "publicly confirmed" giving the inscribed target to the City Manager and the mayor had publicly confirmed that the documents existed, as had the Police Complaint Commissioner. The applicant argued that privacy was not an issue because, among other things, the Chief Constable had given a number of people similar silhouettes and publicly stated that he had given this particular silhouette "as a gift".

The senior adjudicator held that the Board was not required to refuse disclosure of the target silhouette that the applicant requested. Given the extensive publicity surrounding the record and its contents, its disclosure would not unreasonably invade the third party's personal privacy. The senior adjudicator also held that even without that publicity, in light of the contents of the inscription, disclosure of the record would not have been an unreasonable invasion of the Chief Constable's personal privacy.

Order F09-01 – Office of the Premier

The New Democrat Official Opposition caucus requested all records relating to Premier Campbell's question period briefing materials from the recent session of the Legislature.

The Office of the Premier refused the request on the basis that disclosure of the information in dispute, including the factual information, would, if released, disclose advice provided to the Premier as to how to respond to various issues in the Legislative Assembly.

The senior adjudicator held that the evidence demonstrated that the material was compiled, worded and organized for the purpose of advising the Premier on how to respond to questions raised in the Legislature about a wide range of issues. While the records contained factual information, the way the factual materials were assembled constituted advice or recommendations to the Premier as to a "strategical approach" to compiling and framing his responses in a given case, including in a way that promotes the government's position. The senior adjudicator confirmed the decision to withhold the information under s. 13(1) of FIPPA.

Order F09-04 – Ministry of Finance

An applicant requested a contract between the Ministry of Finance and EDS Advanced Solutions Inc. EDS, after having received notice of the request, objected to the release of parts of the contract. The ministry did not accept EDS's position and decided to give partial access to the contract. EDS then requested a third-party review on the ground that the ministry had applied section 21(1) of FIPPA too narrowly. The ministry took the position that it would not respond to any other aspect of the access request until EDS's third-party review was completed. This included information which EDS said it had no objection to the ministry releasing under section 21, as well as information to which it was claimed other disclosure exceptions (sections 15, 17 and 22) applied. The ministry argued that sections 7 and 8 of FIPPA contemplate a public body not responding to the applicant until the completion of a third-party review, with the result that the ministry could wait and invoke other exceptions to disclosure later.

The Commissioner first determined that section 25 of FIPPA did not require the ministry to disclose information in the public interest and that section 21(1) did not require the ministry to refuse to disclose information as claimed by the third-party contractor. Finally, the Commissioner held that the ministry should have proceeded with its response to the applicant by providing access to those parts of the contract that were not protected by section 21(1), as decided by the ministry and as claimed by EDS in its third-party review, or any other relevant exception to disclosure.

5.2 Judicial Reviews

A party who disagrees with an order or decision may request a judicial review by a court. The only judicial review of an OIPC order concluded this year stemmed from a PIPA file originating with a complaint about a company's collection of employee personal information and culminating in separate applications for judicial review – the first following from a decision by the Commissioner not to complete the inquiry, the second following from a subsequent related order:

Cindy Hamilton
REGISTRAR OF INQUIRIES

Judicial Review of Order P07-01– Finning Canada – October 2008

A long-time employee of Finning Canada complained to us about Finning's policy requiring its employees to provide it with their driver abstracts and insurance claim histories annually. Finning argued that the information was necessary for its insurance. When the *Personal Information Protection Act* came into force on January 1, 2004, Finning revised its policy and no longer required insurance claim history information from all employees but only from "directly affected employees".

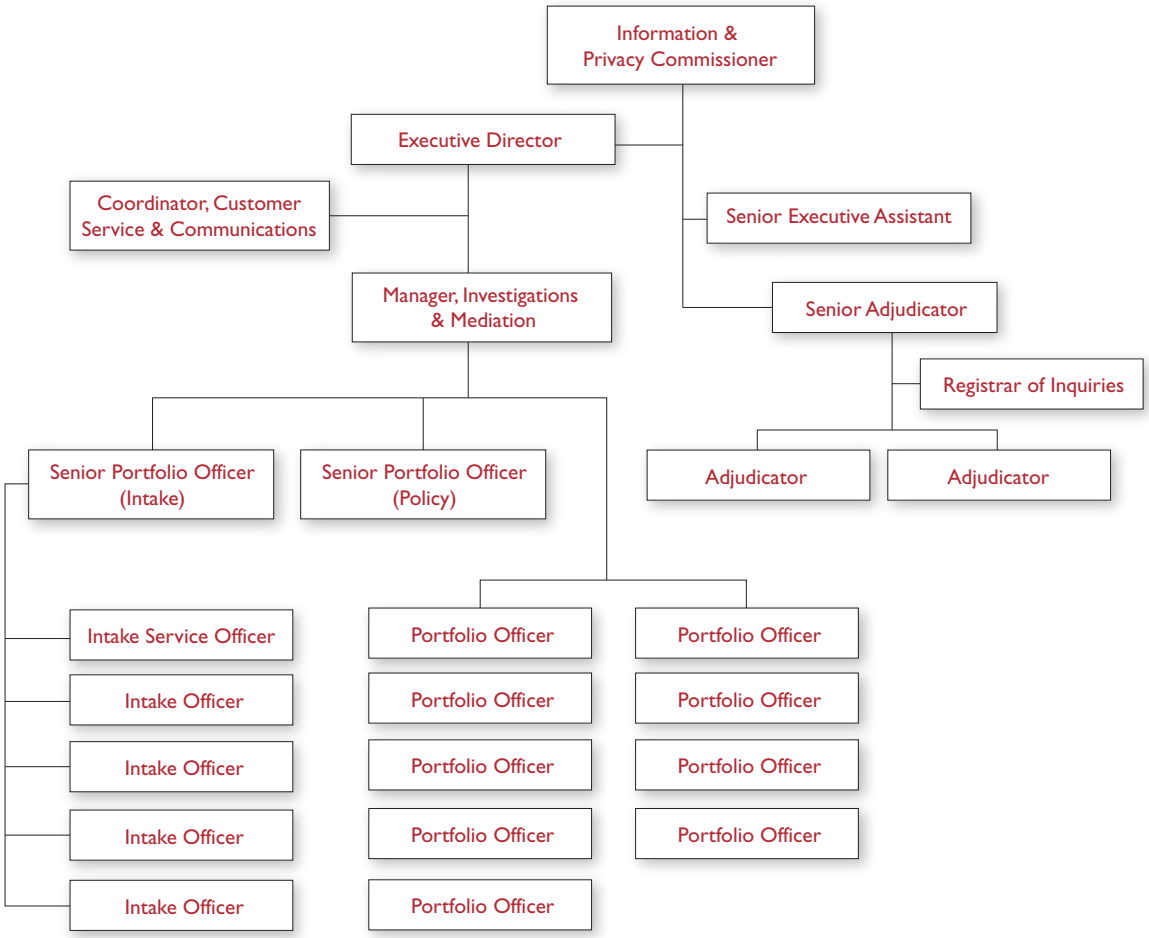
When the complainant objected to being asked for his driver abstract, Finning agreed to accommodate him by requiring that he produce a valid driver's licence only on the rare occasions when he was required to operate a licensed vehicle. His subsequent complaint to us that Finning was not complying with its policy resulted in Decision P07-01, in which the Commissioner declined to complete the inquiry or make an order because the complaint about Finning Canada's collection of driver's licence record abstracts from existing and prospective employees did not concern any information about the complainant.

After the complainant applied for judicial review of this decision, the Commissioner issued Order P07-01, in which he reconsidered his earlier decision. He dismissed the complaint under section 52(1) of PIPA because no personal information of the complainant was involved and the complaint and evidence did not establish or raise reasonable grounds to believe that Finning was not complying with PIPA. The complainant applied for judicial review of this order.

At the judicial review, the Commissioner raised the issue of whether the complainant had sufficient interest in the complaint to warrant an investigation and, if he did not, whether he should be permitted to pursue his complaint on the basis of public interest. For his part, the complainant argued that the accommodation Finning gave him was not permanent and that, if he were to apply for a different position with Finning, he would then be subject to the policy that he complained about.

The court found that the Commissioner was entitled to exercise discretion regarding who should have standing to require an investigation or an inquiry under PIPA and rejected the argument that the Commissioner was incorrect in finding a lack of sufficient interest in the complaint by the complainant. The court also rejected the argument that the complainant had standing on public interest grounds.

Organization Chart



Jacqueline Lebel
INTAKE COORDINATOR

Financial Reporting

1. Authority

The Information and Privacy Commissioner is an independent Officer of the Legislature. The Commissioner's mandate is established under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). FIPPA applies to more than 2,000 public agencies, and accords access to information and protection of privacy rights to citizens. PIPA regulates the collection, use, access, disclosure and retention of personal information by more than 300,000 private sector organizations.

The Commissioner has a broad mandate to protect the rights given to the public under FIPPA and PIPA. This includes: conducting reviews of access to information requests, investigating complaints, monitoring general compliance with the Acts and promoting freedom of information and protection of privacy principles.

In addition, the Commissioner is the Registrar of the Lobbyist Registry program and oversees and enforces the provisions under the *Lobbyists Registration Act*.

Funding for the operation of the Office of the Information and Privacy Commissioner is provided through a vote appropriation (Vote 5) of the Legislative Assembly and by recoveries from OIPC-run conferences. The vote provides separately for operating expenses and capital acquisitions. All OIPC payments are made from, and funds are deposited to, the Province's Consolidated Revenue Fund. Any unused appropriation cannot be carried forward for use in subsequent years.

2. Significant Accounting Policies

These financial statements have been prepared in accordance with Canadian generally accepted accounting principles and reflect the following significant accounting policies:

a) Accrual basis
The financial information is accounted for on an accrual basis.

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

c) Recovery
A recovery is recognized when related costs are incurred.

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

e) Net Book Value
Net Book Value represents the accumulated cost of 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 begins when the assets are put into use and is recorded on a straight-line basis over the estimated useful lives of the assets, as follows:

Computer hardware and software	3 years
Furniture and equipment	5 years

3. Voted, Unused and Used 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. The following is a summary of voted, unused and used appropriations (unaudited):

	2009			2008
	OPERATING	CAPITAL	TOTAL	TOTAL
Appropriation	$3,603,000	$60,000	$2,952,000	$60,000
Other amounts	0	0	0	0
Total appropriation available	$3,603,000	$60,000	$2,952,000	$60,000
Total operating expenses	-$3,481,061	-	-$2,929,643	
Capital acquisitions	-	-$22,766	-	-28,329
Unused appropriation	$121,939	$37,234	$22,357	$31,671

4. Leave Liability

The government changed its policy regarding responsibility for vacation and leave entitlement liability effective April 1, 2006. As of that date, the OIPC was responsible for funding leave expenses from its appropriation. Accumulated leave liability related to vacation and other leave entitlements for the 2008/09 fiscal year was $22,975.41. This was funded in Operating Expenses and was paid through the province's Leave Liability Account.

5. Capital Assets

The following is a summary of capital assets (unaudited):

	2009			2008
	COST	ACCUMULATED AMORTIZATION	NET BOOK VALUE	NET BOOK VALUE
Computer Hardware and Software	$132,682	-$106,140	$26,542	$32,160
Furniture and Equipment	$19,616	-$7,743	$11,873	$5,982
Total	**$152,298**	**-$113,883**	**$38,415**	**$38,142**

6. Leasehold Commitments

The OIPC has a leasehold commitment with Accommodation and Real Estate Services for building occupancy costs and $232,375.25 was paid out in fiscal 2008/09. Payments for office space for the fiscal 2009/10 are estimated at $231,000.00.

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 and joint trusteeship plan, established for certain British Columbia public service employees. The British Columbia Pension Corporation administers the Plan, including paying pension benefits to eligible individuals.

The plan is contributory and its basic benefits are based on factors including years of service and earnings. Under joint trusteeship, the risks and rewards associated with the plan's unfunded liability or surplus is shared between the employers and the plan members and will be reflected in their future contributions.

An actuarial valuation is performed every three years to assess the financial position of the plan and the adequacy of the funding. Based on the results of the valuation, contribution rates are adjusted.

The OIPC also pays for retirement benefits according to conditions of employment for employees excluded from union membership. Payments are made through the province's payroll system. The cost of these employee future benefits is recognized in the year the payment is made.