OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

2009–2010 ANNUAL REPORT

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

2009–2010 ANNUAL REPORT[1]

JULY 2010

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* (FIPPA) guarantees ordinary citizens the right of access to most information (anything recorded in print or electronic form) in the hands of the more than 2,900 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* (PIPA) 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 *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.

CONTENTS

1 REPORT HIGHLIGHTS

The 5,972 files we closed in fiscal year 2009-10 represent an 8% increase over last year. Our caseload has increased by 40% over the past five years. Year after year we find ways to develop new and innovative efficiencies in our handling of files, but public demand for our services continues to grow beyond our ability to respond to all our files in the expeditious and thorough manner they deserve. For example, we managed to close 58% more *Personal Information Protection Act* complaint files and 22% more *Freedom of Information and Protection of Privacy Act* privacy complaint files this year than last, but the number of FIPPA and PIPA privacy complaints received also jumped 18% this year.

British Columbians are becoming ever more concerned about the potential for deliberate or inadvertent misuse of their personal information and ever more vigilant about its protection. No doubt the increased public interest in privacy protection is at least in part the result of frequent publicity about sometimes spectacular breaches of privacy and oftentimes lax security. Whatever the reason, increased public awareness of and concern about privacy protection is a positive development, given the risks of identity theft and other forms of misuse of personal information.

We closed 58% more PIPA complaint files and 22% more FIPPA privacy complaint files this year than last, but the number of FIPPA and PIPA privacy complaints received also jumped 18% this year.

RISK OF PRIVACY EROSION IN GOVERNMENT DATA-SHARING DEEPENS

Widespread electronic sharing of personal information, including the development of a "digital persona" for every citizen, becomes ever more attractive to government for obvious economic and efficiency reasons. In our annual report three years ago, former Commissioner David Loukidelis wrote that it is crucial that privacy protection be built into proposed government data-sharing initiatives from the outset and that, given potential impacts for privacy protection, any initiative to develop a citizen registry of personal information be carefully scrutinized, with meaningful public consultation. Several developments this year suggested that that important message did not have the desired impact and that the privacy risks of data sharing have since become greater rather than smaller.

An investigation by our office of the adequacy of the privacy and security practices of a large e-health data base used by a health authority found that too many staff had access to too much personal information, many of the disclosures of personal information out of the system were unauthorized, and the security of the system was, at the time of the investigation, wholly inadequate. Another investigation of a privacy breach involving two government ministries, affecting the personal information of 1,400 citizens, found that at least 26 different employees had sufficient information to determine that a privacy breach had occurred, yet only two of them recognized that fact, and neither took effective action to alert ministry executives of the breach.

INFORMING THE PUBLIC, RESOLVING DISPUTES, ENFORCING THE LAW

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 and conducting investigations 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.

In 2009-2010, 92% of our review files were resolved by mediation.

MEDIATION SUMMARIES

OK TO WITHHOLD CABINET COMMITTEE DOCUMENT, BUT NOT LETTER DRAFTS FOR PUBLIC BODY

A health authority had to refuse a request to see its business case for a construction project because one of the target audiences for the business case was a Cabinet committee. (SUMMARY 1) However, another public body was not justified in withholding letter drafts from a requester, as the drafts themselves didn't constitute advice or recommendations to the public body, though marginal annotations might have done so. (SUMMARY 2)

EMPLOYEES OBJECT TO NAMETAGS, TENANTS TO PHOTO ID COLLECTION

Employees of a public body lost their fight against wearing nametags because they were considered contact information rather than personal information under FIPPA. (SUMMARY 12) However, in a PIPA file, apartment tenants successfully blocked a landlord's demands to collect their photo ID for "security" reasons. (SUMMARY 17)

FACT OR OPINION? THE KEY QUESTION IN PERSONAL INFORMATION CORRECTION REQUESTS

A credit reporting agency ignored a woman's requests to correct wrong information about her addresses and jobs, but complied after we became involved. (SUMMARY 19) But a patient was unsuccessful in her efforts to force a therapist to correct information on her file because the disputed information was an opinion rather than simply factual. (SUMMARY 20)

2 ACTING COMMISSIONER'S MESSAGE

This year has been a year of significant change and new challenges for the Office of the Information and Privacy Commissioner. In January 2010, David Loukidelis, Information and Privacy Commissioner for the past 10 years, resigned his position as Commissioner to become BC's Deputy Attorney General. His tenure at the OIPC was marked by many significant accomplishments including the release of the *Privacy and the USA Patriot Act* report in October 2004, publication of the first annual report on government's timeliness in responding to access requests, the creation of a standard approach to investigating and responding to privacy breaches that has been adopted across other Canadian and commonwealth jurisdictions, the development of a clear and concise body of law interpreting the meaning of key provisions in the *Freedom of Information and Protection of Privacy Act*, participation in the development and implementation of the *Personal Information Protection Act* and the *E-Health (Personal Health Information Access and Protection of Privacy) Act*, and his work developing privacy frameworks for developing nations on behalf of Canada with the Asia-Pacific Economic Cooperation.

The erosion of privacy protection is nothing new, but the nature and magnitude of the risks to privacy provide increasing cause for alarm.

Our primary challenge during the past year came in the form of growing risks to privacy protection on several fronts. The erosion of privacy protection is nothing new, of course, but the nature and magnitude of the risks provide increasing cause for alarm. They primarily arise from a perhaps inevitable combination of three related trends: the growing proliferation of data-sharing capabilities and practices; a drive to maximize efficiency in data management and sharing for economic and performance reasons; and evidence of a growing attitude in the public sector that, while personal privacy is a commendable goal, its value is perhaps overstated compared to more measurable and desirable indicators related to economic performance. We are encouraged by the fact that in this area there seem to be private sector gains consistent with an understanding that matters of privacy are both important to clients and necessary for efficacious operations.

One of the duties of this office is to comment on the implications for access to information or protection of privacy rights of proposed legislative schemes or programs of public bodies. Unfortunately, during an active spring session, much proposed legislation was referred to us too late for consultation to be meaningful. We plan to continue to work with public bodies to ensure that consultations with this office are timely and meaningful.

Internally, we have been faced with the challenge of effectively coping, with our limited staff resources, with ever-increasing public concern about privacy protection – concern that seems to swell whenever there's a widely publicized breach or other lapse in security. It seems paradoxical that public interest in privacy protection appears to be growing at the very time that institutional vigilance, especially in government, seems to be slipping.

Report of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*

At least once every six years, a special committee of the Legislative Assembly must conduct a comprehensive review of the *Freedom of Information and Protection of Privacy Act*. Since FIPPA came into force in October 1993, there have been two previous reviews (1997-99 and 2003-04). The 2009-2010 Special Committee was appointed in October 2009 and, following a public consultation process, tabled its report in the Legislature on May 31, 2010.

I was very pleased to have the opportunity to present the submission of the Office of the Information and Privacy Commissioner to the Committee at its last public hearing on March 31. My colleagues Catherine Tully, Celia Francis and Helen Morrison also participated in the presentation. The Committee gave us an attentive hearing and engaged in useful discussion. Of our 22 recommendations, 16 were endorsed by the Committee in its report.

It is my sincere hope that government will act quickly to implement the Committee's recommendations with respect to the appointment of a Government Chief Privacy Officer, routine proactive disclosure of government documents and a public consultation process on data sharing. When implemented, these measures will go a long way towards resolving significant issues in the areas of both access and privacy protection.

The Wider the Sharing, the Broader the Risk: Protecting Personal Information

Ready access to citizens' personal information can immensely increase the efficiency of delivering public services at the lowest possible cost. From that perspective, technological advances that facilitate the electronic collection, storage and sharing of personal information – cumulatively building "digital personas" of every individual – appear to be economically attractive.

One of the most prominent recent examples of major data organization and sharing initiatives has been the introduction of eHealth systems throughout health authorities in the province. In March 2010, we concluded a three-year investigation of the adequacy of privacy protection in the Vancouver Coastal Health Authority's community-based electronic health record system. The Primary Access Regional Information System (PARIS) has roughly 4,000 users – VCH staff and contractors – involved in the delivery of a wide range of community health services outside of acute care hospitals. The personal information contained in PARIS is highly sensitive and includes, for example, diagnoses as well as the case notes of physicians, nurses and counselors.

Our investigation found the protection of personal information in PARIS to be inadequate. Major deficiencies include an access model that is team-based rather than role-based, with far too many users having access to too much personal information;

unauthorized sharing of personal information outside the health authority; substandard security protection given the sensitivity of the information; and indefinite storage of records that are neither archived nor destroyed when no longer needed for the provision of care. The problems we identified were a result not of software deficiencies but of inadequate attention to privacy considerations in the process of making PARIS operational in community care programs.[1]

The efforts of the Ministry of Health Services to implement the E-Health Act have been somewhat disappointing and have not lived up to the initial promise of openness and transparency and robust privacy protection for all data flows of personal health information through databases of the ministry and health authorities.

We have been closely monitoring implementation of the *E-Health (Personal Health Information Access and Protection of Privacy) Act*, which was passed with our support in 2008. To date, the efforts of the Ministry of Health Services have been somewhat disappointing and have not lived up to the initial promise of openness and transparency and robust privacy protection for all data flows of personal health information through databases of the ministry and health authorities. The ministry has only applied the legislation to a new provincial database containing lab results that will be accessed by health care providers. This database, known as the Provincial Laboratory Information Solution, is the first repository of the interoperable Electronic Health Record that is funded, in part, by Canada Health Infoway. Our office is a member of a Privacy Forum of Canada Health Infoway that shares information about how privacy issues are being addressed by provincial governments.

Last year in his annual report message, the former Commissioner noted that the provincial government was moving forward with a number of programs that involve the more widespread disclosure of personal information across government and across agency boundaries in the name of service delivery. He urged that "the demands of efficiency and supposed improvements in service quality not diminish our privacy inappropriately." We commented this year on a number of proposals that continue to cause significant concern that technologies are enabling, and in some sense driving, the creation of more and more personal information databases. The collection and matching of pieces of disparate information about each citizen creates a digital persona of each of us that we may be entirely unaware of. It will exist throughout our lives and may affect decisions that public bodies make about us. The importance of building structure, accountability and transparency around this process is vitally important and urgent.

In this regard, we are actively monitoring the new Integrated Case Management system that will be used by both the Ministry of Housing and Social Development and the Ministry of Children and Families. Among other things, we wish to ensure that there is a role-based access model in place that is based on need-to-know and least privilege principles and that the security framework, audit policy and privacy breach policy are adequate. We look forward to reviewing the privacy impact assessment for this project.

1 Investigation Report F10-02 http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF10-02.pdf.

Expediency Trumping Privacy – A Dangerous and Unnecessary Trend

Building secure privacy protection into the design stage of systems, quite apart from simply being a legal requirement, can avoid the far greater future expense needed to contain leaks and rebuild public trust in the event of abuses or inadvertent leaks.

It's easy to jump to the conclusion that the need to protect privacy impedes the design of systems intended to maximize the efficient use of personal information in the delivery of services. In fact, the contrary is true. Building secure protection into the design stage, quite apart from simply being a legal requirement, can avoid the far greater future expense needed to contain leaks and rebuild public trust in the event of abuses or inadvertent leaks.

The trend to allow expediency to trump privacy considerations is particularly worrisome in situations where information is sensitive or clients are vulnerable. The sharing of health information, referred to above, is another good example of this. Patients receiving the services of health authorities, fearful of jeopardizing their ability to receive prompt and comprehensive treatment, are ill-placed to question how well their information is protected. In a very different type of investigation, we looked at the Bar Watch requirement for bar patrons to provide, and have recorded, their driver's licence information to enable bars to discourage the presence of disruptive clientele. Our investigation concluded that Bar Watch could achieve the same purpose without such an intrusive requirement. The assumption that many clients would be willing to forgo privacy rights in order to receive services, while quite possibly correct, was unwarranted insofar as there was no need to brush privacy considerations aside to achieve the desired end.

The issue of data sharing across government formed the focus of government's submission to the Special Committee to Review FIPPA that met in the fall of 2009 and the early spring of 2010. The submission states, "Leveraging current technological developments is key to meeting public expectations for service access and delivery and providing world-class citizen centric services, but this requires integrated and coordinated information sharing and information management."[2] The government's submission goes on to recommend a series of changes to FIPPA that would profoundly limit the nature and extent of the privacy protections.

In our response we pointed out that FIPPA is sufficiently broad and flexible to accommodate data sharing projects within the currently privacy protection framework.[3] FIPPA is a fundamentally sound piece of legislation based on internationally recognized privacy principles. We will continue in our oversight role to provide government with guidance on how these projects can be designed and implemented within the current privacy framework. But we continue to be very concerned about these trends toward the creation of digital personas. We will also work to raise public awareness of these issues and to ensure that citizens actively participate in any changes to the existing privacy regime.

There is little need to alter a law that already works. Instead, greater emphasis should be placed on working with the law to secure a reasonable balance between protection of and efficient use of information, incorporating protections adequately into the design of information management systems, and ensuring that users of those systems understand their responsibility to protect personal information. An investigation we completed this

2 Government Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act, March 15, 2010 found at: http://www.leg.bc.ca/foi/organizations.htm

3 Submission of the A/Information and Privacy Commissioner to the Special Committee to Review the Freedom of Information and Protection of Privacy Act, March 15, 2010 found at: http://www.leg.bc.ca/foi/organizations.htm . Transcript of oral submission available at: http://www.leg.bc.ca/cmt/39thparl/session-2/foi/hansard/F00331a.htm

spring was particularly revealing on the latter point. After a ministry employee took the personal information of 1,400 citizens, the loss of the information was not discovered until the RCMP located the documents in the home of the employee. At least 26 different employees had sufficient information to determine that a privacy breach had occurred, yet only two of them realized that a breach had occurred, and these two failed to take effective action to ensure that the matter was brought to the attention of the appropriate executive member within their ministry.[4] The consequence was that the ministry suffered not only the expense of repairing the breach but also a considerable amount of bad press. Privacy protection need not be a headache to organizations if the basics of the law are simply understood and applied as standard practice.

There is little need to alter a law that already works. Instead, greater emphasis should be placed on working with the law to secure a reasonable balance between protection of and efficient use of information, incorporating protections adequately into the design of information management systems, and ensuring that users of those systems understand their responsibility to protect personal information. Privacy protection need not be a headache to organizations if the basics of the law are simply understood and applied as standard practice.

Back to the Basics: Why Privacy Matters

The legislated right to privacy protection in both the public and private sector, in the *Freedom of Information and Protection of Privacy Act* and the more recent *Personal Information Protection Act*, constituted recognition of hard-won rights that many countries still lack, but are nevertheless fundamental human rights. The right to privacy has long been recognized as a component of the right to liberty. It is not something that should be treated lightly or acknowledged only when it doesn't appear to get in the way of efficient delivery of services. More to the point, privacy and efficient delivery of services are not antithetical objectives; properly planned, they complement one another very well indeed.

FIPPA has now been in operation almost two decades, while PIPA has just passed its sixth anniversary. Both pieces of legislation were warmly received when they came into force not only by the public but also by public bodies and organizations that recognized the new laws as both fair and progressive. Clearly, there continues to be strong public interest in and ever increasing awareness of the value of privacy protection. It is perhaps not surprising that the same level of enthusiasm does not universally continue at the organizational level, yet it is important for public bodies and private sector organizations to honour our privacy law both in principle and practice. The difficulty of doing so is often greatly exaggerated.

Timeliness Update: Ministry Responses to Access Requests

Last year we reported on the results of our first compliance report cards for ministries covering calendar year 2008. We identified serious problems with the provincial government's timeliness in responding to access to information requests. We advised that following the initial report, we would begin reporting on the fiscal year beginning with the period April 1, 2009 to March 31, 2010. We now have in our possession statistical reports provided by ministries. Once we have had the opportunity to conduct some verification of the statistics, we will prepare a second public compliance report. We anticipate that this report will be ready by the summer of 2010.

4 Investigation Report F10-01 http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF10-01.pdf.

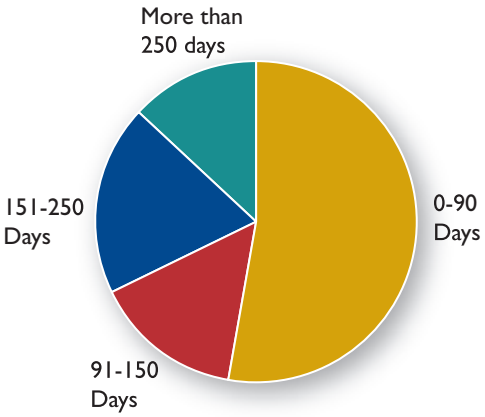
Assessing OIPC's Performance

For the first time last year we reported on our own performance. Below is a report on our performance this year. While we have met our target for responding to review requests within 90 business days or fewer, we have been unable to meet the 150 and 250 business day targets. The same pattern emerges in our response times to complaints. This year we closed a total of 1,143 complaints and reviews, up slightly over last year. In addition, the total number of files received this year was up by 440 files or almost 10%. This occurred with no change in the number of staff at the OIPC.

Our main strategies to deal with our high caseload issue have focused on ensuring that cases that do not need to proceed through to a full investigation or mediation are identified and resolved early. While these strategies have helped us to manage our growing caseload, our ongoing challenge is simply that we lack the staff to investigate and mediate all the matters that require resolution within our targeted timelines.

Matters closed in the first 90 business days for reviews and 120 business days for complaints are generally closed by the Early Resolution Officer or by the Intake Team. Any file that takes longer than that to resolve is a file that has to await assignment to the next available investigator or mediator.

Over the past three years, while our caseload has continued to increase, the number of investigators/mediators has remained constant. In response we have adopted a number of strategies in an attempt to reduce our processing time and to deal with our ever-increasing caseload. Our main strategies to deal with this caseload issue have focused on ensuring that cases that do not need to proceed through to a full investigation or mediation are identified and resolved early. Strategies include the development of the early resolution process which involves assigning most files first to the Early Resolution Officer, who identifies issues, gathers relevant records and attempts, where possible, to find an early resolution to matters. Another strategy is to delegate broader duties to the intake team, who are able to resolve more straightforward matters within weeks of receipt. Matters that require immediate attention such as deemed refusals, privacy breaches, and



HOW OLD WERE THE (FIPPA & PIPA) CLOSED REVIEW FILES DURING 2009-2010 WHEN THEY WERE CLOSED?

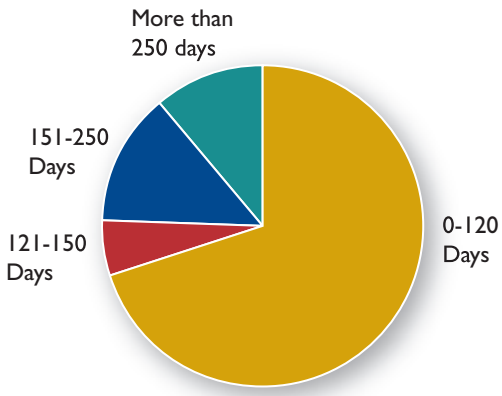
	TARGET	ACTUAL
90 business days or fewer	**50%**	316/599 = **53%**
150 business days or fewer	**75%**	410/599 = **68%**
250 business days or fewer	**95%**	521/599 = **87%**

comments on draft legislation are sent immediately to an investigator for comment. By contrast, matters where the complainant has failed to first raise the issue with the public body or organization are referred back to the complainant to pursue with the public body or organization first.

While these strategies have helped us to manage our growing caseload our ongoing challenge is simply that we lack the staff to investigate and mediate all the matters that require this service within our targeted timelines. For calendar year 2008-2009 there were an average of 174 files per month awaiting assignment for investigation or mediation. In 2009-2010 that number had increased to 226 files per month awaiting assignment. An experienced investigator/mediator can resolve an average of 110 files in a year. Therefore, it would take an additional two full-time, experienced investigator/mediators one year to reduce the backlog to zero. Next year, without additional resources, in all likelihood this number will continue to increase.

HOW OLD WERE THE (FIPPA & PIPA) CLOSED COMPLAINT FILES DURING 2009-2010 WHEN THEY WERE CLOSED?

	TARGET	ACTUAL
120 business days or fewer	**60%**	342/544 = **63%**
150 business days or fewer	**75%**	370/544 = **68%**
250 business days or fewer	**95%**	492/544 = **90%**



Office of the Registrar of Lobbyists

Under the *Lobbyists Registration Act* (LRA) I am appointed as the Registrar of Lobbyists. As a result of significant amendments that came into effect on April 1, 2010 the LRA was improved and strengthened.

To meet these new responsibilities and promote province-wide compliance with the new rules, a number of key organizational changes were made. The Office of the Registrar of Lobbyists (ORL) was formed and a new position of Deputy Registrar of Lobbyists was created to support the operational plan to establish a separate unit to implement the significant changes to the LRA and the longer-term strategic plan to promote and enforce province-wide compliance with the LRA using full-time dedicated staff. The ORL staff created a suite of compliance tools, including policies and procedures, FAQs and advisory bulletins, and free workshops were held around the province.

Our strategy for securing compliance with the new lobbyist registry rules will mainly focus on education and support. Part of our compliance message is to de-stigmatize the act of lobbying and rebrand it as a normal and legal part of the democratic process.

A new online-registration system, eighteen months in the making, was successfully launched on March 31, 2010. I would like to acknowledge the significant contributions made by the Ministry of Attorney General, Sierra Systems and ITI Technologies in its success.

A significant on-line media strategy was delivered, and the ORL launched its first website, which can be found at www.lobbyistsregistrar.bc.ca

Our strategy for securing compliance with the new rules will mainly focus on education and support, and as such, our outreach plans will extend well into the new fiscal year. Part of our compliance message is to de-stigmatize the act of lobbying and rebrand it as a normal and legal part of the democratic process. Lobbying is not a crime, but failing to register is.

This is the last year the ORL message will be contained in the OIPC Annual Report. The amendments to the Act now require the Registrar of Lobbyists to publish his or her own Annual Report, and the first will be published in 2011, reflecting on the events of this year.

Conclusion

My tenure as the Acting Information and Privacy Commissioner lasted through five very busy months and included making detailed submissions to the Special Committee, commenting on numerous significant legislative proposals, completing two major privacy investigation reports, beginning an in-depth review of a large database, implementing the changes to the Lobbyists Registration Act and completing this annual report. This work would not have been possible without the hard work and dedication of the staff of the office. I am grateful to all of the staff for their assistance and professionalism during my time as the Acting Information and Privacy Commissioner.

PAUL D. K. FRASER, Q.C.

3 THE YEAR AT A GLANCE: A STATISTICAL OVERVIEW OF OUR ACTIVITIES IN 2009–10

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 and Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). Explanatory notes following each table clarify terms used in the table and the significance of various totals.

Table 1 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 2009 – 31 MARCH 2010

FILE TYPE	RECEIVED 09/10	CLOSED 09/10	RECEIVED 08/09	CLOSED 08/09
Information Requested/Received				
Requests for information	3658	3654	3309	3311
Read and file	128	122	91	92
Media queries	60	61	29	27
Freedom of information requests for OIPC records	10	9	9	9
Requests for Review				
Requests for review of decisions to withhold information	562	599	630	655
Applications to disregard requests as frivolous or vexatious	6	5	6	4
Complaints				
Complaints about non-compliance with FIPPA or PIPA	573	544	487	452
Reviews/investigations Declined				
Non-jurisdictional	48	46	50	50
No reviewable issue	152	150	129	133
Requests for Time Extension				
By public bodies/organizations for time extension	353	345	277	276
By applicants for time extension to request a review	29	32	34	31
Reconsideration of Decisions				
Internal reconsideration of OIPC decisions	25	26	10	7
Adjudication	2	3	2	2
Files Initiated by Public Bodies/Organizations				
Privacy impact assessments	12	8	3	4
Public interest notification	12	10	16	17
Notification of privacy breaches	71	62	79	91

TABLE 1. *continued*

FILE TYPE	DISPOSITION RECEIVED 09/10	CLOSED 09/10	RECEIVED 08/09	CLOSED 08/09
OIPC-Initiated Files				
Investigations	3	5	14	15
Projects	36	31	22	20
Reviews of proposed legislation	42	39	57	60
Policy or Issue Consultations	104	113	127	114
Public Education/Outreach				
Speaking engagements by OIPC staff	59	70	74	76
Conference attendance	12	12	24	25
Meetings with public bodies/organizations	12	25	35	28
Site visit by Commissioner to public bodies/organizations	0	1	6	5
Other	1	0	10	14
Totals	**5970**	**5972**	**5530**	**5518**

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 599 requests for review we completed this year included 566 under FIPPA (Table 2) and 33 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 544 complaint files closed this year included 397 under FIPPA, of which 310 related to access to information and 89 related to protection of privacy (Tables 4 and 5). We also closed 145 PIPA complaints (Table 7).

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 first notify us.

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.

TABLE 2. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY TYPE, 2009–10

	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	22	54	0	0	0	7	0	2	**85**
Deny Access	0	67	0	0	0	12	0	5	**84**
Notwithstanding (s. 79)	0	1	0	0	0	0	0	1	**2**
Partial Access	0	297	0	0	0	20	1	31	**349**
Refusal to Confirm or Deny	0	7	0	0	0	0	0	0	**7**
Scope	0	7	0	0	0	1	0	1	**9**
Third Party	0	21	0	0	0	1	1	7	**30**
TOTAL	**22**	**454**	**0**	**0**	**0**	**41**	**2**	**47**	**566**

TABLE 2 DEFINITIONS:

Consent order: OIPC order, following deemed refusal and with agreement of parties, specifying final date for public body response.
Deemed refusal: Failure to respond within required timelines (s. 7)
Deny access: All information withheld from applicant (ss. 12-22)
Notwithstanding: Conflict between FIPPA and other legislation (s. 79)
Partial access: Some information withheld from applicant (ss. 12-22)
Refusal to confirm or deny: Refusal by public body to confirm or deny the existence of responsive records (s. 8)
Scope: Requested records not covered by FIPPA (ss. 3-4)
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, 2009–10

	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	119	0	0	0	6	0	2	**127**
Vancouver Police Department	0	28	0	0	0	4	0	2	**34**
Ministry of Public Safety and Solicitor General	4	18	0	0	0	4	0	3	**29**
Vancouver Island Health Authority	2	21	0	0	0	1	0	4	**28**
Fraser Health Authority	0	16	0	0	0	2	0	5	**23**
City of Vancouver	1	18	0	0	0	0	0	0	**19**
Ministry of Attorney General	3	10	0	0	0	0	0	5	**18**
Vancouver Coastal Health Authority	0	11	0	0	0	0	0	3	**14**
Ministry of Housing and Social Development	6	7	0	0	0	1	0	0	**14**
Ministry of Health	0	12	0	0	0	0	0	2	**14**
Top 10 totals	**16**	**260**	**0**	**0**	**0**	**18**	**0**	**26**	**320**
All Other Public Bodies	6	194	0	0	0	23	2	21	**246**
TOTAL	**22**	**454**	**0**	**0**	**0**	**41**	**2**	**47**	**566**

TABLE 3 EXPLANATORY NOTES:

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

TABLE 4. DISPOSITION OF FIPPA ACCESS COMPLAINTS, BY TYPE, 2009–10

	DISPOSITION									
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED BACK TO PUBLIC BODY	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY/REPORT ISSUED	REPORT ISSUED	TOTAL
Adequate Search	14	19	0	6	37	1	0	0	0	**77**
Duty Required by Act	50	16	11	13	43	11	0	2	0	**146**
Fees	25	12	1	1	8	3	0	0	0	**50**
Time Extension by Public Body	4	21	1	8	0	3	0	0	0	**37**
TOTAL	**93**	**68**	**13**	**28**	**88**	**18**	**0**	**2**	**0**	**310**

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, 2009–10

	DISPOSITION									
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED BACK TO PUBLIC BODY	WITHDRAWN	DECLINE TO INVESTIGATE	NOTICE OF REPORT ISSUED	REPORT ISSUED	TOTAL
Collection	3	7	0	0	6	2	0	0	0	**18**
Correction	1	4	0	0	6	1	0	0	0	**12**
Disclosure	5	6	2	5	17	4	2	2	0	**43**
Retention	0	2	0	0	1	1	0	0	0	**4**
Use	0	3	1	1	0	0	0	0	0	**5**
Protection	2	1	0	1	1	0	2	0	0	**7**
TOTAL	**11**	**23**	**3**	**7**	**31**	**8**	**4**	**2**	**0**	**89**

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. FIPPA ACCESS AND PRIVACY COMPLAINTS BY PUBLIC BODY, 2009–10

	NUMBER OF FILES CLOSED										
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
Insurance Corporation of BC	4	3	0	4	5	1	0	1	9	1	**28**
Ministry of Public Safety. and Sol. Gen	6	0	1	2	9	1	0	0	4	1	**24**
Ministry of Transportation & Infrastructure	2	0	0	0	3	14	0	0	0	0	**19**
WorkSafeBC	3	1	2	5	8	0	0	0	0	0	**19**
Vancouver Island Health Authority	8	0	1	2	5	0	0	1	1	0	**18**
Ministry of Health Services	3	0	0	2	7	0	2	0	2	0	**16**
Ministry of Housing and Social Development	7	0	0	0	5	1	1	0	1	0	**15**
Ministry of Children & Family Development	0	1	1	2	3	2	0	0	3	2	**14**
City of Vancouver	3	1	0	0	5	2	0	0	1	0	**12**
University of BC	0	1	0	0	9	0	0	0	0	0	**10**
Vancouver Coastal Health Authority	2	0	0	2	5	0	0	0	1	0	**10**
Top 10 totals	**41**	**8**	**5**	**20**	**66**	**21**	**3**	**3**	**22**	**4**	**193**
All Other Public Bodies	36	10	7	23	80	29	4	1	15	1	**206**
TOTAL	**77**	**18**	**12**	**43**	**146**	**50**	**7**	**4**	**37**	**5**	**399**

TABLE 7. DISPOSITION OF PIPA COMPLAINTS, BY TYPE, 2009–10

	DISPOSITION								
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED BACK TO ORGANIZATION	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	TOTAL FILES CLOSED
Adequate Search	1	3	0	1	2	1	0	0	**8**
Collection	5	4	0	6	14	0	0	1	**30**
Correction	3	1	0	0	3	1	0	0	**8**
Disclosure	7	9	1	1	15	1	0	0	**34**
Duty Required by Act	30	4	0	2	9	4	0	0	**49**
Fees	1	0	0	0	0	1	0	0	**2**
Protection	3	1	0	1	2	1	0	0	**8**
Retention	1	2	0	0	0	0	0	0	**3**
Use	0	2	0	0	0	1	0	0	**3**
TOTAL	**51**	**26**	**1**	**11**	**45**	**10**	**0**	**1**	**145**

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, 2009–10

	DISPOSITION				
TYPE	MEDIATED	WITHDRAWN	OTHER DECISION	NOTICE OF INQUIRY ISSUED	TOTAL
Deemed Refusal (PIPA)	18	1	0	0	**19**
Deny Access	3	3	0	0	**6**
Partial Access	4	1	0	0	**5**
Refusal to Confirm or Deny	0	1	0	0	**1**
Scope	2	0	0	0	**2**
TOTAL	**27**	**6**	**0**	**0**	**33**

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).

4 INFORMING THE PUBLIC

Catherine Tully
EXECUTIVE DIRECTOR

For a variety of reasons, we consider it very important to keep the public informed about the rights and responsibilities conferred by the two laws we administer – the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA) – and to participate in (or lead or organize) conferences and workshops with a privacy or access component. Many of our staff make great efforts to carve out time for public education activities in addition to their day-to-day roles as mediators, investigators, intake officers and senior managers.

The following is a brief catalogue of a few of the key reasons why we consider our public information role an important component of our work and why we do our best to accommodate requests to deliver addresses or otherwise participate in events focusing on privacy protection or access to information rights:

- We have a statutory obligation for monitoring how FIPPA and PIPA are administered to ensure that its purposes are achieved. Part of that obligation includes informing the public about FIPPA and PIPA.
- Access to information and protection of personal privacy are fundamental rights recognized in law but constantly under threat from competing objectives such as economic expediency. We need to ensure that, as much as possible, the word gets out that these are rights for good reason and deserve to be respected consistently.
- FIPPA and PIPA, though written with considerable care and clarity, are complex pieces of legislation both because there are many necessary exceptions to the general rights of access and privacy protection and because several provisions have nuanced meanings that require a very clear understanding (for example, what does consent for collection of personal information really mean and when is it necessary?)
- Public interest in privacy protection is constantly growing, partly as a result of frequent publicity about security lapses and partly because of widespread fear of identity theft in a digital age, and there is a strong public appetite for information about the role our office plays, how we handle disputes, our relationship with other jurisdictions such as the federal Privacy and Information Commissioners, and practical steps people can take to protect their personal information.
- The more people understand about their privacy and access rights and responsibilities as ordinary citizens or institutional representatives, the greater the likelihood that potential disputes will be avoided or resolved before they ever land on our doorstep. When we receive complaints or requests for review, we place great emphasis on resolving them early and expeditiously at the Intake stage or through quick work by our Early Resolution Officer. In a very real sense, our work

Access to information and protection of personal privacy are fundamental rights recognized in law but constantly under threat from competing objectives such as economic expediency. We need to ensure that, as much as possible, the word gets out that these are rights for good reason and deserve to be respected consistently.

Angela Arkell
INTAKE SERVICE OFFICER

in informing the public takes our "early resolution" process a step ahead – if, by providing clear information and analysis at lectures and conferences, we provide the understanding needed for people to resolve access and privacy issues before they might otherwise feel the need for assistance, we at the same time increase our own efficiency by reducing our complaints and requests for review numbers, thereby helping to keep our very high caseload manageable.

In 2009-2010, we reached at least 1,800 people through addresses to audiences such as the following:

- Vancouver City Hall
- Law Society of BC
- TELUS Ambassadors West
- University of Victoria third year journalism class
- Co-operative Housing Federation of BC
- PIPA 2009 Conference
- Fraser Health Authority
- Simon Fraser University
- Clinical Research Professionals of BC
- Tsawwassen First Nation
- Thompson Rivers University
- 2009 Canadian Association of Journalists Conference
- Canadian Bar Association
- Reboot Conference
- Canadian Life & Health Insurance Association
- College of Physicians and Surgeons
- Canadian Bar Association Administrative Law Presentation
- Fasken Martineau (Continuing Legal Education for Counsel)
- Canadian Bar Association FOI & Privacy Section AGM
- University of Victoria
- BC Privacy Professionals Association
- Data Privacy Day Conference
- Canadian Bar Association Joint Privacy and Employment Law Section Meeting
- Condominium Home Owners Association Vancouver AGM
- Victoria Foundation
- Coastal Water Suppliers Association Conference
- College of Occupational Therapists of BC
- Vancouver Island University Vancouver City Hall
- Law Society of BC
- Canadian Manufacturers and Exporters Association
- BC NDP Opposition Research Team
- College of Occupational Therapists of BC
- International Association of Privacy Professionals

Inform Yourself Online About Your Rights and Our Role

Almost two decades in the business have provided us ample opportunity to develop a clear interpretation of the laws we administer and to develop online resources designed to foster a clear public understanding of how the laws work too. The following resources on our website are worth a look for anyone seeking a general understanding of FIPPA or PIPA or wanting specific information about a problem:

FIPPA

Policies and Procedures Guide – how we deal with FIPPA issues brought to our attention, and what you need to know to expedite resolution of your problem: http://www.oipc.bc.ca/advice/FIPPA_Policies_and_Procedures(May2009).pdf

Sectional Index – a section-by-section annotation of OIPC orders arising from FIPPA inquiries. The order numbers in boldface indicate leading orders illuminating the interpretation of each section:

http://www.oipc.bc.ca/index.php?option=com_content&view=article&id=87&Itemid=71

PIPA

A Guide to PIPA for Businesses and Organizations

http://www.oipc.bc.ca/pdfs/private/a-_GUIDE_TO_PIPA%283rd_ed%29.pdf

FAQs about PIPA – privacy rights and beyond: http://www.oipc.bc.ca/index.php?option=com_content&view=article&catid=17%3Aprivate-sector-pages&id=71%3Aprivate-sector-g-frequently-asked-questions&Itemid=77

Sectional Index – http://www.oipc.bc.ca/index.php?option=com_content&view=article&catid=20%3Aorders-&id=121%3Aprivate-sector-g-sectional-index&Itemid=85

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

5 RESOLVING PROBLEMS

Pat Egan
SENIOR PORTFOLIO OFFICER

The OIPC has many tools at hand for resolving issues that arise in the application of BC's freedom of information and protection of privacy laws. We act as a source of information for anyone needing assistance in the interpretation of the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA) or simply wanting practical advice on how most effectively to obtain access to information or protect personal information. We act as a sounding board for public bodies and private sector organizations seeking feedback on whether proposed policies or programs are likely to be compliant with FIPPA and PIPA. We review all bills tabled in the Legislative Assembly to determine whether they have any FIPPA or PIPA implications and, if so, we try to ensure that all potential conflicts have been foreseen and addressed. We give media interviews and travel, when time permits, to make presentations in different parts of the province to foster understanding of our privacy and access laws.

Our primary purpose in these efforts is to ensure that FIPPA and PIPA function as smoothly as possible, with maximum understanding of and compliance with the law. When misunderstandings and disputes do occur, we bring other skills to bear to try to remedy the situation. Our team of Intake Officers fields calls, questions and complaints and, if possible, tries to resolve a problem in a single phone call by providing the information or advice needed to defuse a potential conflict at the outset. If one or more issues still remain unresolved, Intake transfers the file to a Portfolio Officer, who will identify the key issues, analyze the legal requirements, and attempt a resolution through informal mediation.

Our team of Intake Officers fields calls, questions and complaints and, if possible, tries to resolve a problem in a single phone call by providing the information or advice needed to defuse a potential conflict at the outset.

To expedite resolutions as much as possible once Intake has referred a file to our investigations team, a Portfolio Officer acting as an Early Resolution Officer first reviews the file to determine whether a "quick fix" might be possible through a simple phone call or two. The better we are able to "cut to the chase" through such file management techniques, the greater our ability to keep up with a very large and ever growing caseload. Summaries 15 and 19 in the following pages illustrate the type of shortcuts we achieve through the early resolution process.

MEDIATIONS AND INVESTIGATIONS

If all of our early resolution attempts are unsuccessful, Portfolio Officers are assigned the files to either conduct a mediation of a review or an investigation of a complaint.

The amount of work required for a mediation may range from a quick call to extensive legal research and patient negotiations with affected parties that could extend through

Early Resolutions for Increased Efficiency

Our caseload is so high (a 40% increase over the past five years) that we are always looking for new ways to improve our efficiency and speed up the resolution process. We have no control over the numbers of problems that come our way from people exercising their legal rights, and our complement of staff does not automatically rise to deal with swelling numbers. What we can control, at least to some degree, is the time spent on each file and our rapidity of response to straightforward cases. As a result, we are constantly innovating in the belief that only by experimenting with different efficiency techniques can we find out what truly works in our unique circumstances.

Although it remains impossible, given our very limited staff resources and ever-rising caseload numbers, to meet the targets we set for file resolution, the following combination of methods has helped us to at least keep the backlog somewhat manageable:

1 ***Intake Shortcuts to Success.*** In many agencies with a dispute resolution mandate, the role of Intake is simply to field complaints and forward them to investigators for much later review. We take the view that if a problem has a simple solution, it should be addressed on the spot rather than languishing somewhere in a slush pile. Consequently, our Intake team takes a proactive role resolving problems that can be fixed with a call or two. In doing so, they benefit from their own considerable experience in problem resolution as well as a working familiarity with our legislation and the network of other agencies involved in the administration of FIPPA and PIPA. On top of this, Intake resolves many non-jurisdictional issues by referring callers (or people who contact us by email or letter) to the right destination.

2 ***Next Opportunity: Early Resolution.*** The issues raised by complaints and requests for review can be relatively simple or tremendously complex. Complex files can take months to resolve, and sending simple files to the back of a long queue is in no one's best interest. The nature of access to information and privacy protection disputes is such that a delayed resolution is of little use to many applicants and complainants for whom a favourable result is pointless if not quick. Three years ago we decided to designate an Early Resolution Officer whose job it would be to review files assigned by Intake to Portfolio Officers and separate out those that might expeditiously be resolved. The experiment was a resounding success, with the result that single-issue files tend to be resolved very quickly by the Early Resolution Officer.

3 ***Early, Early Resolution:*** Public Information about Rights and Opportunities for Resolution. Well designed and easily accessible websites are a crucial component to problem resolution in the 21st century. The OIPC website tries to provide clear and easily understood explanations of people's rights under FIPPA and PIPA, steps they can take to resolve matters before approaching our office, and how to make the best use of the services we provide. We've had our hiccups making the website as user-friendly as possible, but it remains a top priority for us. The other important way we inform the public about our role and their rights (and responsibilities) is by organizing conferences on privacy and access to information, responding to requests for informal talks and formal lectures, and participating on panels discussing existing laws and opportunities for improvement in privacy protection and rights of access (see chapter 4 on this topic).

weeks or months . The Portfolio Officer conducting the mediation might express an opinion about how the law (FIPPA or PIPA) applies to the issue at hand, while emphasizing that a mediation is simply that – an effort to assist the parties to mutually agree upon a solution (which itself might be suggested by the Portfolio Officer).

When a public body withholds information from someone who has requested access under FIPPA, it must provide reasons for doing so, with specific reference to the legislative exemption on which it relies.

The great majority of our mediations lead to successful outcomes. However, in the event that one or more parties is unable to agree to a solution and expresses the wish for a formal ruling on the matter, the Portfolio Officer will then explain how to request an inquiry by the Commissioner or one of our Adjudicators. The Adjudicator conducting the inquiry has the benefit of a Statement of Facts and Issues prepared by the Portfolio Officer but otherwise has no knowledge of what transpired during mediation. In addition, any parties who might be affected by the outcome of the inquiry are provided an opportunity to make written submissions. The Adjudicator's order, including a clear factual and legal rationale, is publicly available and is posted on our website.

Whereas requests for review focus on decisions responding to requests for access to information, complaints to our office deal with other aspects of FIPPA, such as delays in responding to access requests, fees charged for retrieving and preparing information, or improper collection, use or disclosure of a complainant's personal information. Portfolio Officers have the delegated authority to investigate complaints and to make findings and conclusions that resolve the matter.

This chapter of the annual report includes illustrative summaries of mediations and investigations we conducted this year under FIPPA and PIPA. The following chapter presents summaries of selected orders.

5.1 FIPPA Requests for Review

FIPPA provides a general right of access to information in the custody or control of public bodies. Public bodies are defined in Schedule 1 of FIPPA and specifically listed in Schedules 2 and 3, and in general terms include most agencies of the provincial and municipal levels of government.

Sections 12 through 22 of FIPPA describe a number of exceptions to the general right of access. When a public body withholds information from someone who has requested access under FIPPA, it must provide reasons for doing so, with specific reference to the legislative exemption on which it relies. Typically, that involves making reference to one of the exemptions described in sections 12 through 22 as justification for severing or withholding part or all of a record.

A requester who has been denied access to some or all of the information requested may ask us to review the decision of the public body to deny access. The summaries below describe mediations we conducted to resolve disputes arising from the application of sections 12 through 22.

Cabinet and Local Public Body Confidences (s. 12)

Summary 1 Health Authority Withholds Records Destined for Cabinet Committee Consideration

A man requested access to records relating to the business case prepared by a health authority for the construction of a large hospital project. The applicant had originally submitted the request to Partnerships BC because the project was being built as a Private-Public Partnership (P3). Partnerships BC, which assisted the health authority in the early stages of the project, no longer had custody or control of the responsive records and transferred the request to the health authority.

The health authority denied the applicant access to the business case, citing its obligation under section 12(1) of FIPPA not to disclose information that would reveal the substance of deliberations of Cabinet or of its committees. Section 12(1) is a mandatory exception to disclosure, requiring a public body to: "refuse to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees, including any advice, recommendations, policy consideration or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of it members." The applicant asked us to review the health authority's decision.

Court decisions have provided useful guidance for the interpretation of section 12. In *Aquasource Ltd. v. British Columbia (Information and Privacy Commissioner)* [1998], B.C.J. No. 1927, the court concluded that the scope of information that fell under section 12(1) was broader than just the arguments put forth pro and con that resulted in a decision. The test that results from this decision is whether the information in dispute formed the basis for Cabinet's deliberation. In other words, documents prepared for Cabinet's consideration or considered by Cabinet in making its decision also fall under section 12(1).

In this case, the public body showed that large capital projects must be approved by a Cabinet committee and that the business case had been submitted to a Cabinet committee for approval. On this basis, we told the applicant that it was unlikely he would receive additional information by pursuing formal adjudication, and he decided not to pursue the review any further.

Caitlin Lemiski
EARLY RESOLUTION OFFICER

Policy Advice, Recommendations, or Draft Regulations (s. 13)

Summary 2 Advice to a Public Body Doesn't Automatically Include Drafts of Letters

Following an argument with an employee of a public body on public body property, a woman made an FOI request for all of the information the public body had kept about the incident. The public body released a copy of a letter that had been addressed to her regarding the incident but withheld six other pages under section 13 of FIPPA, claiming the pages were advice or recommendations to the public body.

Suspicious about the nature of the withheld information, the woman asked us to review the severing. We obtained copies of the withheld records and found that they consisted

FIPPA TIP FOR PUBLIC BODIES

When applying the section 13 exemption, consider carefully whether the text in question constitutes advice or a recommendation. Background information or drafts of a final letter that has since been sent generally will not pass the test, so judicious severing may be required. (Summary 2)

entirely of draft versions of the letter that had been released. We advised the public body that, in the past, the Information and Privacy Commissioner had held (in Order 00-27) that draft letters are not automatically considered to be advice or recommendations just because they are drafts, and that that only those parts of the letter that actually consisted of advice or recommendation, such as margin notes containing substantive changes or edits, could be withheld.

We suggested that the public body minimally sever the draft letters so that only those parts that could be considered advice or recommendations were removed, and release the remainder. The public body did so, enabling the applicant to see that the six pages that had been withheld were simply drafts of the letter she had already seen.

Legal Advice (s. 14)

Summary 3 Price Hike Raises Lessee's Suspicions of City Motives

A woman who entered into negotiations with a municipality for the renewal of a land lease for a long-established business with a charitable component was taken aback by the tough bargaining position adopted by the municipality. In her opinion, her relationship with the municipality had always been on good terms, yet it was now insisting on a price that far exceeded anything paid in the past.

Curious as to why the municipality was being so hard-nosed, and wanting to satisfy herself that the process had been fair, she asked for copies of all records relating to the contract, including details of matters considered by the public body in its negotiations with her. On receiving the municipality's response, the woman was surprised that large portions of the records had either been withheld entirely or severed extensively. She asked us to review the municipality's response to her access request.

Our review of the records revealed the portions that had been withheld from the applicant and showed that the municipality had applied the exemptions contained in sections 14, 17 and 22 of FIPPA in support of its decision to withhold information.

A few members of the public had sent unsolicited views, pro and con, on their perception of the value to the community of the services offered by the applicant's business. The municipality severed information from these communications under section 22 of FIPPA, which requires that the head of a public body must refuse to disclose personal information if the disclosure would be an unreasonable invasion of a third party's personal privacy. Under that section, the public body had severed information such as names, addresses and other references regarding members of the public that might identify them or reveal information about their individual circumstances. The applicant accepted that this information could arguably be withheld.

Section 14 provides that a public body may refuse to disclose information that is subject to solicitor-client privilege. With the agreement of the municipality, we reviewed the records subject to section 14 as part of the mediation and described to the applicant the nature of the records without revealing their content. We were satisfied from our review

that the records were written communications of a confidential nature between the public body and its lawyer for the purposes of seeking and giving legal advice and accordingly were properly withheld. The applicant accepted our opinion.

The bulk of the records had been withheld from the applicant under section 17 of FIPPA. This section permits a public body to refuse to disclose information that could reasonably be expected to harm the financial interests of a public body, including information about negotiations carried on by a public body. We concluded that disclosure of much of the withheld information would not harm the interests of the public body. In fact, the contrary appeared to be true, insofar as the information revealed what appeared to be a thorough and logical approach to negotiations. The municipality appeared to agree with us that, if anything, revealing this information would show it had acted in a fair and determined way in protecting the public interest, and decided to release substantially more information. This was sufficient for the applicant, who considered the matter resolved.

The municipality also explained, in the course of our review, that the reason for its negotiation of a land lease renewal price far in excess of previous arrangements simply was rooted in a legal requirement. As a result of further consideration the municipality had come to a decision that the business was just that – a business rather than a charitable entity – and accordingly the municipality was required by the *Community Charter* to charge market rates for the lease.

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

Summary 4 Public Body's Proactive Resolution Makes Light Work for OIPC

A city denied a request for access to information about a piece of land that the city had leased, citing section 17 of FIPPA. After the applicant requested a review of that decision, the city advised us that, in addition to section 17 – a discretionary exception that authorizes a public body to withhold information the disclosure of which could reasonably be expected to harm the financial or economic interests of a public body – it was considering adding section 21 of FIPPA. Section 21 is a mandatory exception that requires a public body to withhold information that, if disclosed, would be harmful to the business interests of a third party.

As required by section 23 of FIPPA, the city then notified the third party of the access request. It also notified the applicant that it was providing the third party with the opportunity to make representations concerning disclosure, as the third party's interests could be affected by disclosure.

Without our knowledge, the city subsequently reconsidered its initial decision. Because section 17 is a discretionary exception, the city decided it no longer needed to rely on section 17 to withhold the information. Further, the city determined that it was no longer required to refuse disclosure under section 21 because, as a result of the third party notification, the third party had consented to the release of the information. Then the city gave the applicant access to the records she had requested.

While the release of information might not have occurred had the applicant not asked us to review the city's decision to withhold the information, the matter was resolved before the file was assigned to a Portfolio Officer. Once the request for review was submitted, the city took the lead in reconsidering its initial decision and making appropriate notifications, the result of which was the release of the information the applicant had requested.

This is a good example of a public body taking the initiative to resolve a matter, with minimal involvement by us.

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

Summary 5 Third Party Consents to Release of Contract Information

FIPPA TIP FOR PUBLIC BODIES

The section 21 exemption cannot generally be applied to text that has been written into a contract or other agreement between a public body and another party as a result of mutual negotiation of the language to be included. (Summary 5)

A public body received a request for access to a contract for services between the public body and a third party. The third party objected to the release of the contract and asked us to review the public body's decision to release the contract. The third party suggested that releasing the contract would harm its business interests and therefore section 21 of FIPPA required the public body to withhold it.

Section 21 is a mandatory exception that requires a public body to withhold information that, if disclosed, would be harmful to the business interests of a third party. However, section 21 creates a three-part test, each element of which must be satisfied before a public body is required to refuse to disclose information. As stated in paragraph 58 of Order F08-22:

> Section 21(1) has now been analyzed and applied in many orders in which it has been held that this exception does not require a public body to refuse access to the mutually generated contents between public bodies and third parties.

As a result of our mediation, the third party agreed that much of the information could be released, and so the public body released this information to the individual who had made the access request. While it was our view that section 21 would likely not apply to most of the information that remained in dispute, the individual who had made the access request was satisfied with the release and agreed that it was not necessary to pursue the matter any further.

The matter was concluded when all parties were satisfied with the result of the mediation.

Disclosure Harmful to Personal Privacy (s. 22)

Summary 6. Distraught Parents Seek Explanation for Daughter's Death

A couple spent the night in a hotel. When the boyfriend awoke the next morning, he discovered his girlfriend was not breathing and called 911. The paramedics and police responded quickly but were unable to revive her. The cause of death was determined to be a drug overdose.

The parents subsequently requested a copy of the police report in an effort to gain more insight into what had happened that fateful evening. The police department gave them a

copy of the police report after severing all information about the boyfriend and his actions that evening, citing section 22(1) of FIPPA. As the couple had spent the whole evening together, the information about them recorded in the police report was so comingled that it would have been difficult to release information regarding the daughter without releasing personal information about the boyfriend.

The concerned parents asked our office to review the police report to see if any additional information could be released to them. Subsequent to our involvement, the boyfriend wrote to the police department giving them his consent to share his information with the parents in an effort to answer their questions regarding what had happened that night. The consent enabled the police department, under section 22(4) of FIPPA, to release additional information to the parents regarding their daughter's death, and they were satisfied with this additional information.

Summary 7 Dad Denied Access to Daughter's College Enrolment Records

A non-custodial father requested access to his grown daughter's college enrolment records and a list of courses in which she was enrolled. We agreed with the college's severing pursuant to section 22(3)(d) of FIPPA, concluding that the father was not entitled to this information unless he provided the college with evidence of the consent of his adult daughter.

Section 22(3)(d) of FIPPA upholds the proposition that the disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if the personal information is related to that person's educational history. Section 3 of the Freedom of Information and Protection of Privacy Regulation outlines who may exercise access rights for young people under the age of 19. If the person is 19 years old or older and is able to make his or her own decision as to who has access to their own personal records, then that adult's consent must be obtained. In this case, the father had not obtained his daughter's consent and the college rightly refused to release the responsive records to the applicant.

FIPPA TIP FOR REQUESTERS

If you are requesting information about a person who is young (under the age of 19), you don't automatically have a right to the information because of a close relationship. Only the parent or guardian has the right to request the personal information of someone under 19 – and then only if the young person is incapable of exercising that right himself or herself. (Summary 7)

Summary 8 Adoptee Asks for Information about Deceased Birth Parents

A woman who had been adopted as an infant asked a public body for her adoption file. The public body released a large portion of the file but severed out some personal information relating to her birth parents under section 22 of FIPPA, on the assumption that a complete release might be an invasion of the parents' personal privacy. The woman asked us to review that decision, pointing out that the adoption file dated from the 1950s and her birth parents had been deceased for many years.

In the past, the Information and Privacy Commissioner has held (in Order 02-26) that an individual retains a reduced privacy interest in personal information even after death, the degree of the interest depending on the sensitivity of the information and the age of the record.

Justin Hodkinson
PORTFOLIO OFFICER

After reviewing the withheld records, we recommended that the public body consider releasing several pieces of information that were not sensitive. It did so, but continued to withhold some information considered to be of a more sensitive nature. The applicant accepted our opinion that her birth parents still had a privacy interest in the records that remained severed due to their sensitive nature.

Relationship of FIPPA to Other Acts (s. 79)

Summary 9 Legislative Override Bars OIPC Review of Denial of Access

A woman asked the Family Maintenance Enforcement Program for copies of records related to her file. Program staff explained to her that the *Family Maintenance Enforcement Act* contains a non-disclosure provision that applies notwithstanding the access rights contained in section 4 of FIPPA. As a result, they denied her request for access, and she asked us to review that decision.

Section 79 of FIPPA states that if there is a conflict between FIPPA and a provision in another Act, FIPPA applies unless the provision in the other Act expressly states that it applies despite FIPPA. Section 43(1) of the *Family Maintenance Enforcement Act* states: "Despite the *Freedom of Information and Protection of Privacy Act*, a person must not disclose information obtained under this Act…" There are some exceptions to this non-disclosure provision, but they do not apply to an individual making an access request under FIPPA.

In this case, the non-disclosure provision of the *Family Maintenance Enforcement Act* overrides the access rights in FIPPA. Since section 43(1) applies to all Family Maintenance Enforcement Program records, our office lacked authority under FIPPA to review the Program's decision.

5.2 FIPPA Complaints

Portfolio Officers conduct investigations into access and privacy complaints. Investigations can be straightforward or complicated, ranging from simply interviewing the complainant and public body and gathering relevant records to conducting onsite visits, interviewing witnesses, testing database security and gathering documentation for third parties. Most investigations take only a few weeks, but more complicated investigations, such as the recent investigation into a large e-health system, can take months and, on occasion, years. The summaries below illustrate some of the most common complaint investigations into such matters as the adequacy of searches, privacy breaches and the fairness of fees.

Complaints involving particularly complex issues or matters of significant public concern may lead to major complaint investigations the reports of which are posted on our website (click on Orders, Investigations and Decisions). Summary 10 provides a synopsis of one such investigation this year (Investigation Report F09-01 on our website).

Summary 10 Jury Check Lands Defence Lawyer in Hot Water

The Insurance Corporation of British Columbia (ICBC) notified us that a lawyer it had retained to defend an insured driver in personal injury litigation had asked the ICBC claims adjuster handling the file to conduct checks on the trial jurors to find out if any of them had previous ICBC claims. The adjuster checked the jurors in ICBC's databases and provided claims information to the lawyer. When ICBC management found out, ICBC's in-house counsel appeared before the trial judge and told him what had happened. ICBC also notified the jurors and apologized to them for its actions. The personal injury case was settled and the trial was discontinued.

Following a request from the minister responsible for ICBC, we agreed, with certain conditions, to conduct an investigation into the disclosure by ICBC of the personal information of jurors in court proceedings. In addition, ICBC conducted its own internal investigation and identified five other cases of jury checking in recent years. We conducted a detailed privacy assessment in order to determine if ICBC had sufficient safeguards in place to prevent the inappropriate disclosure of personal information by ICBC claims adjusters to external defence counsel. While ICBC had policies in place to prohibit jury checking, we concluded that they hadn't been effective in preventing it entirely. We recommended that ICBC focus on more specific training for claims adjusters and better communication and awareness of ICBC's privacy policies for external defence counsel.

Duty to Assist Applicants (s. 6)

Summary 11 Delay in Responding Adds to Grievance about Fee Estimate

A man asked the Office of the Premier (OOP) for all background papers and analysis that led to the cabinet decision to reorganize BC Ferries. He also requested a fee waiver, arguing that access to the records was in the public interest. OOP responded with a fee estimate for the cost of producing the records, denying the fee waiver request on the grounds that the responsive records were not of current public interest or the subject of public debate. The man then complained to our office about both the denial of his fee waiver request and the length of time that OOP was taking to respond to his request.

There is a two-step process for determining whether a fee should be waived in the public interest. A public body must determine whether or not the requested records relate to a matter of public interest and, if they do, decide if the applicant should be excused from paying all or part of the fees.

The applicant claimed that the privatization of BC Ferries had been a topic of recent public debate and that the public is concerned that the government is increasingly putting the expenditure of public money beyond public scrutiny. He argued that the public is also concerned about the accountability of the government regarding privatization, outsourcing and the awarding of contracts involving large amounts of public funds. He also expressed concern about the removal of BC Ferries from the scope of FIPPA, thereby limiting the access to information the public used to enjoy. Thirdly, he argued that the

public should be given an opportunity to inform themselves of the changes that occurred with BC Ferries and the outsourcing of government services.

We concluded that the decision to privatize BC Ferries had been the topic of recent and ongoing public debate and, after reviewing several hundred pages of responsive records provided by OOP, found that none of the records were "administrative" type records, for which it could be argued a fee waiver should not be provided.

The coastal ferry system is an essential component of British Columbia's transportation system. A large number of BC residents and its tourism industry rely on the services provided by BC Ferries, and the governance of BC Ferry Services Inc. has a large and direct impact on the lives of many British Columbians. We concluded that the change in policy to privatize a formerly government controlled entity was a matter of public interest and that responsive records would contribute to the public's understanding of how this decision was made.

We also concluded that the question of the privatization of BC Ferries closely relates to an examination of how the BC provincial government is allocating financial or other resources and that the disclosure of the records would contribute to the development or public understanding of, or debate on, an important policy, law, program and service and would shed light on how the BC government is allocating its financial resources.

The above factors satisfied us that the records were in the public interest and that the dissemination of the information by the applicant could contribute to the ongoing public debate and understanding about the privatization process of BC Ferries as a non-governmental body.

As a result of OOP's delays in processing the applicant's request, we found that OOP had not satisfied its section 6 duties under FIPPA. Not meeting a time limit is a factor in fashioning a remedy under section 58(3)(c) of FIPPA.

Having concluded that a fee waiver of $390 would not place an unreasonable burden on the public body, we recommended that OOP reimburse the fee to the applicant, and it agreed to do so.

Use of Personal Information (s. 32)

Summary 12 Foster Parent Applicant Objects to Check of Her Childhood Contacts

A woman who applied to the Ministry of Children and Family Development (MCFD) to be a foster parent signed a basic consent form giving MCFD the right to do a "prior contact check" on her. In a prior contact check, MCFD looks at any previous history between a person and MCFD, such as previous foster parent experiences.

In this case, ministry staff also looked at the woman's childhood MCFD file, along with her mother's MCFD file. When the woman learned this, she complained to us about what she considered the excessive scope of the background check.

Section 32 of FIPPA allows a public body to use personal information in a defined set of circumstances, one of which is "if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use" (section 32(b)). In this case, MCFD acknowledged that the consent form the applicant signed did not indicate how broad the background check would be or how MCFD would use the information they had on the applicant. Although it seemed reasonable to us for MCFD to look at foster parent applicants' childhood contacts with MCFD, informed consent was required to meet the section 32 requirement, as that particular use of personal information would not fall under section 32(a) or (c).

To further complicate matters, the complainant had left part of the form uncompleted, insofar as she had not ticked the boxes indicating the types of information to which her consent applied. MCFD staff had failed to notice that no boxes had been ticked.

We concluded that the complaint was substantiated as section 32 requirements for the use of personal information had not been met. MCFD agreed to revise their consent form to indicate how an applicant's personal information would be used, with an eye to ensuring informed consent for any use MCFD might consider necessary.

FIPPA TIP FOR EMPLOYEES

Many public servants are justifiably concerned about maintaining a low profile and not revealing too much personal information to members of the public. Remember, though, that FIPPA's definition of personal information specifically excludes contact information, which is the information that members of the public need to know in order to be able to contact the right person to discuss or obtain a service provided by government. Contact information includes only the essentials – it does not, for instance, include an employee's photo. (Summary 13)

Disclosure of Personal Information (s. 33)

Summary 13 Employees Lose Fight against Wearing Nametags

A public body decided to instruct senior employees in direct contact with the public to wear nametags. Although the nametag included the name of the employee, the public body's website information included the names, positions, responsibilities, locations, phone numbers and email addresses of each of its senior staff.

Concerned that clients could use their names to locate their home phone numbers and addresses, some employees asked the public body to rescind the requirement to wear nametags and to remove their name from the website. In response to the employees' argument that the public body was disclosing too much personal information by revealing their names, the public body countered that it was simply contact information and was thus excluded from the meaning of personal information under FIPPA.

Schedule 1 of FIPPA differentiates between personal information and contact information. "Personal information" means recorded information about an identifiable individual other than contact information. "Contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

The purpose of disclosing contact information is to enable communication between the public and service providers. Contact information was exempted from the definition of personal information to allow disclosure of this information without bringing the public body into conflict with FIPPA.

FIPPA TIP FOR REQUESTERS

The first three hours spent locating and retrieving records when you make an access request are free. After that, the public body can charge you. That's one good reason to keep access requests as focused as possible. If the public body does charge you, you may still have the option to prove your request is in the public interest and that you're able to widely disseminate the information (to enable public review), but you'll need to make that case convincingly to justify a fee waiver. (Summaries 14 and 15)

The FIPPA definitions addressed all of the concerns brought by the complainants to our attention except one – the description of employee responsibilities, which is personal information not included in the definition of contact information. Section 33.1 (1) of FIPPA describes circumstances when a public body may disclose personal information inside or outside Canada. Section 33.1(1)(a.1) allows a public body to disclose personal information described in section 22(4)(e). Section 22(4)(e) authorizes a public body to disclose an employee's position and function.

As the legislation left no room for ambiguity, we concluded that the public body was authorized to disclose the employees' contact information and responsibilities by having the employees wear a nametag and posting senior staff contact information and responsibilities on its website.

Fees (s. 75)

Summary 14 Critic of Public Art Installation Probes Approval Process

Recent public art installations in a coastal city received a wildly mixed response and generated considerable controversy. In an effort to better understand the process of awarding public commissions to artists and to contribute to the public debate, a citizen requested copies of all artist submissions from the two most recent public art projects.

The city asked for payment of a fee of $254.50, according to the schedule of fees listed in section 7 of the Freedom of Information and Protection of Privacy Regulation, to cover the estimated cost of the search and photocopying. The man paid the fee under protest so he could get the records, but also asked the city for a fee waiver.

Section 75(5)(b) of FIPPA provides that the head of a public body may waive fee payment if the record "relates to a matter of public interest, including the environment or public health or safety". The city denied the fee waiver request stating that it did not see how the records were a matter of public interest or how the citizen could widely disseminate the information. (Order No. 332-1999 described a process for determining whether records relate to a matter of public interest, part of the test being whether dissemination of the records could yield a public benefit.)

A local newspaper subsequently published a feature article about public art projects in the city and used some of the records the citizen had received from the city and shared with the paper. After we became involved and the newspaper article was published, the city conceded that the records could be seen to relate to a matter of public interest and that the citizen had successfully disseminated the information. It then granted a fee waiver and gave the complainant a full refund.

Summary 15 Reviewing Records in Person avoids High Fee

A labour organization asked a public body for preliminary records related to sharing services and procurement. When the public body responded with a fee estimate of several hundred dollars, as authorized by section 75(1) of FIPPA, the labour organization asked for a fee waiver on the basis that access to the records was in the public interest.

The public body denied the request, noting that the records were only drafts and had not been used for making a decision. It also cited the age of the records as a factor for denying the fee waiver request.

After the labour organization complained to us about the public body's denial of the fee waiver, our Early Resolution Officer talked to the representative of the labour organization to explore the possibility of practical alternatives to a full-scale complaint investigation. On its own initiative, the labour organization told us that it had decided to contact the public body to see if it could review the records in person in order to avoid paying a fee. The public body accepted that proposal, and after viewing the records, the labour organization decided to withdraw its complaint as its needs had been met.

Troy Taillefer
PORTFOLIO OFFICER

5.3 PIPA Requests for Review

Access to Personal Information (s. 23)

Summary 16 Agency with Possession but Not Control Justified in Denying Access to Emails

A non-profit agency's Board of Directors made a decision about a woman that she believed was unjustified. Dissatisfied with the Board's explanation about the reasons for the decision, she wanted to determine exactly what the Board members had discussed.

She began by writing to another agency where one of the Board members was employed, requesting copies of emails sent or received by the Board member that mentioned her name. Under PIPA individuals have the right, with some exceptions, to access their own personal information. However, section 23(1)(a) of PIPA restricts the right of access to personal information that is in the control of an organization.

The woman argued that because the emails she requested were stored on the email server of the agency where the Board member worked, that agency had control of the information. Our review confirmed that the Board member did use her email account at work to conduct some of her Board business, but that was not enough to determine who had control of the information. In order to establish who has control of personal information it is necessary to consider all aspects of the information's creation, use and maintenance. Some of these factors include:

- Did the Board member create the personal information as part of her Board duties?
- Does the employer have a right of possession of the personal information?
- Does a contract specify the information as being under the control of the employer?
- Does the content of the information relate to the employer's mandate?
- Has the employer relied upon the personal information to a substantial extent?
- Is the information integrated with other information held by the employer?

Based on this analysis, we concluded that possession of the information by the employer did not equate to control as defined by PIPA. The Board member's employer was

PIPA TIP FOR INDIVIDUALS

If you believe an organization has recorded wrong information about you, you have every right to request a correction, and the organization must honour that request if you make a reasonable case, and at the very least annotate your request if the correction doesn't seem warranted. The right to obtain a correction only applies to factual errors and omissions, not to opinions expressed about you by an organization. (Summaries 19 and 20)

not required to provide access to emails created by its employee in her capacity as a Board member for another agency.

5.4 PIPA Complaints

Limitations on Collection of Personal Information (s. 11)

Summary 17 Landlord's Demand for Tenants' Photo ID Hard to Justify

Some tenants in an apartment building complained to us about the landlord's insistence on collecting their photo ID. The landlord described to us a variety of reasons for requiring this type of personal information, including the potential need to verify a tenant's identification in an emergency or when someone has locked themselves out, or to do a credit check. However, when we questioned whether photo ID was really necessary for those purposes, the landlord agreed it probably wasn't.

PIPA balances the need for individuals to protect their personal information and the need for organizations to collect personal information for business purposes. Section 11 of PIPA limits the collection of personal information for purposes that a reasonable person would consider appropriate in the circumstances and that fulfil the purposes of the organization. The test of reasonableness is used to balance the competing interests.

We appreciated the landlord's cooperation with our investigation and its willingness to amend its practices by curtailing its requests for tenants' photo ID. This resolved the matter and we had no need to take any further steps.

Quite apart from PIPA's prohibition of the collection of unnecessary personal information, there's another practical reason for limiting collection to absolutely necessary information. Section 34 of PIPA requires organizations to make "reasonable security arrangements" to protect personal information from "unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks". The more personal information collected, the greater the risk to the organization. Since personal information that is collected must be protected, the risks can be reduced by collecting less personal information and only that which is essential.

Disclosure of Personal Information without Consent (s. 19)

Summary 18 Sharing Employee Information without Consent OK (with Conditions)

A business hired a third party service to take over certain human resources functions such as managing WorkSafe BC claims and conducting the necessary follow-up with injured workers. The service provider claimed to be able to provide some injured workers with shorter wait times for certain medical coverage. Employees were given the option to opt out of the program without any negative implications.

To enable the service provider to perform the contracted functions, the business shared with it relevant personal information of its employees, including name, address, social insurance number, BC Care card number, date of birth, telephone number and some medical history.

A former employee subsequently complained that the business had inappropriately disclosed his personal information to the service provider. Section 19(2) of PIPA provides that an organization may disclose an employee's personal information without his or her consent if it is reasonable for the purposes of managing an employment relationship between an organization and an individual.

We concluded that section 19(2) applied in this instance, so the complaint was not substantiated. We also concluded, however, that section 19(2) would not have authorized the employer to share with the service provider the personal information of employees who had elected to opt out of the program.

Right to Request Correction of Personal Information (s. 24)

Summary 19 Credit Reporting Agency Accused of Ignoring Correction Request

A woman who asked a credit reporting agency for a copy of her credit report noticed several errors, including addresses where she had never lived and employment she had never held. After receiving no response from the credit reporting agency to her written request for correction, she complained to our office about the failures to correct the errors in her personal information.

Section 24 of PIPA authorizes individuals to ask organizations to correct their personal information. Although PIPA elsewhere specifies that an organization must respond within 30 days to a request for access to an individual's personal information, it sets no time limit for a response to a request for correction. However, section 24 does require an organization, once satisfied on reasonable grounds that the information should be corrected, to do so. If the organization does not consider a correction to be warranted, it must at least annotate the personal information with the correction that was requested but not made.

When our Early Resolution Officer called the credit reporting agency to see if the matter could be simply resolved, the agency began to investigate and quickly discovered that a computer error had caused information about another person with a similar name to appear on the woman's credit file. The credit reporting agency fixed the errors so that only the woman's own information appeared on her credit file and mailed her an updated copy of her credit report so she could see that the changes had been made.

Summary 20 Therapist Not Required to Correct Written Opinion

A woman wrote to her therapist asking him to correct an error in her personal information. Under section 24(1) of PIPA, an individual may ask an organization to correct their personal information under the control of the organization. If the organization believes on reasonable grounds that there is an error in the complainant's personal information, it must correct the error and notify each organization to which the information has been disclosed during the previous year.

Section 24 only requires an organization to correct factual errors or omissions in personal information, such as an incorrect date of birth. An organization is not required to

correct information in the form of an opinion expressed by the organization in applying its knowledge about a subject – for example, a doctor's diagnosis or a police summary of an incident. However, the organization must annotate the request for correction to the complainant's file.

In this case, the complainant disagreed with the therapist's recommendations but did not point out any factual errors in the recommendation or even explain what information appeared to be incorrect. Since the therapist did not know what personal information was at issue, he was not required to make either a correction or an annotation to the file.

Protection of Personal Information (s. 34)

Summary 21 Laptop Theft from Doctor's Office Jeopardizes Patient Information

Staff at a doctor's office called the police and our office on discovering the theft of a laptop containing patient personal information. On beginning an investigation of the privacy breach, we quickly ascertained that personal information stored on the laptop's hard drive had not been encrypted.

Section 34 of PIPA requires an organization to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks. 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 of those affected is required, and develop prevention strategies.

In this case, the ability of the physician's office to contain the breach was limited because the laptop was not recovered. However, they anticipated the risk of hurt, humiliation and damage to reputation and decided to notify the affected individuals. They also replaced the laptop computer with a desk top computer and encrypted any data stored on the hard drive. We concluded that the physician's office had taken adequate steps to remedy the breach and to prevent it from recurring in the future.

Generally, if an organization has a secure network server, it is preferable to store personal information there rather than on the hard drive of a laptop or desktop computer. However, where an organization finds it necessary to store personal information on a hard drive, the only reasonable safeguard in most instances is encryption. Cable locks are also a good tool to assist with physical security.

6 ENFORCING THE LAW

Celia Francis
SENIOR ADJUDICATOR

Anyone who requests a review under the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act* and is unhappy with the outcome of mediation may request a formal inquiry. If the OIPC accepts the request, the Commissioner or Adjudicator conducting the inquiry distributes to all parties to the dispute the statement of facts and issues prepared by the mediator, invites submissions from the disputants and any potentially affected third parties, and prepares a written, legally binding order that analyzes the facts, issues and application of the law and provides a clear rationale for the decision.

Any party affected by an OIPC order who disagrees with an order has the option to apply to the Supreme Court of British Columbia for a judicial inquiry. There is a similar process called a hearing for those who are not satisfied with the results of investigations into their complaints.

The summaries below provide a sampling of the 35 FIPPA and four PIPA orders the Commissioner and adjudicators issued during the 2009-10 fiscal year.

6.1 FIPPA Orders

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

Order F10-06 — Ministry of Agriculture and Lands

The applicant, the T. Buck Suzuki Environmental Foundation, requested audit information that the ministry gathered from fish farms. Among other things, the audits contained information relating to sea lice counts of farm fish and results from the testing of fish the fish farms turned over to the ministry. The ministry refused the request on the basis that the fish farms supplied the information in confidence and disclosure could subject the fish farms to various harms if disclosed.

The adjudicator ordered disclosure of the information. He found that the fish carcasses turned over to the ministry for testing did not constitute the supply of information under section 21 of FIPPA. Moreover, he found, the fish farms did not supply information explicitly or implicitly in confidence and, in the event it did, the ministry had failed to prove that its disclosure could reasonably be expected to cause harm. The Adjudicator rejected the ministry's argument that the applicant would use disclosed information out of context, thereby harming the fish farms' operations. If this were a basis for withholding records, he said, one could easily envision very little disclosure of information by public bodies that are, in many cases, concerned with how information might be used and viewed by members of the public.

Fees (s. 75)

Order F09-05 — Law Society of British Columbia

The applicant, First Canadian Title, made two requests for a variety of records on title insurance and other matters spanning the five years before its request. The Law Society issued fee estimates totalling just over $117,000 for responding to the requests. The applicant complained to the OIPC about the amounts of the fee estimates, including the Law Society's characterization of First Canadian Title as a "commercial applicant". It also complained about the Law Society's "delay" in responding.

Mediation led to the consolidation of the requests and a revised fee estimate of $11,000. The applicant paid the estimated fee and the Law Society disclosed records in phases over ten months. The Law Society's final processing costs were about $27,000 and it charged the applicant this amount. The applicant remained dissatisfied with both the amount of the fee and the pace of disclosure and these matters proceeded to a hearing.

The Senior Adjudicator found that the applicant was a "commercial applicant", which meant the Law Society could charge the applicant actual costs for providing certain services. However, she also found that the Law Society had included certain charges in its fee estimate which were not allowable under FIPPA or its Regulation. She therefore ordered the Law Society to re-calculate the fee in accordance with guidelines set out in the Order. She also reduced the revised fee by 20% because, among other things, the Law Society did not take steps earlier to expedite processing of the request.

Definitions (Schedule 1)

Order F09-08 — Corporation of the Village of Burns Lake

A journalist and a town councillor from the Village of Burns Lake requested records from the Village relating to several entities connected with the Burns Lake Community Forest Lands in the northern interior of BC. The Village transferred the request to a corporate entity known as ComFor because it said ComFor had control of the records. The Village created ComFor, owned 100% of its shares and appointed all of its directors. ComFor in turn provided management and administrative services to a group of four companies all of which it controlled through 100% share ownership. ComFor and the four other companies argued they were neither specifically listed under Schedule 2 of FIPPA nor captured by the definition of "local government body" under Schedule 1.

The Adjudicator found that the requested records were subject to FIPPA. Although ComFor's officers were not directly appointed by the Village, the Village's role as sole shareholder, including the power to appoint and remove its directors, provided a significant nexus between the Village's authority and the officers of ComFor such that in conjunction with other factors present, ComFor's officers were chosen or appointed under the authority of the Village. It followed from this that the four companies ComFor controlled were also subject to FIPPA.

6.2 PIPA Orders

Provision of Consent (s. 7)

Order P09-01— Cruz Ventures Ltd. (doing business as Wild Coyote Club)

The complainant visited Vancouver's Wild Coyote Club, an establishment licensed to serve liquor. At the door, Wild Coyote employees asked the complainant to produce his driver's licence. The employees then swiped the licence through a card reader and required the complainant to have his digital photograph taken. The complainant did not receive what he considered to be a reasonable explanation as to why his personal information was being collected and later complained to us about the club's practices.

In his order, the Commissioner acknowledged that licensed establishments should be able to preserve a safe environment for customers and to identify those individuals who have been determined to be violent or otherwise undesirable for re-entry from a safety perspective. Nevertheless, he found that section 7(2) of PIPA does not authorize the organization to require customers to consent to collection of the scope of personal information (for example, driver's licence numbers), as doing so did not further this safety purpose. He also found that no persuasive reason related to improved customer safety had been provided for a licensed establishment's retention of information relating to customers who are not involved in violent incidents. As such, the collection of personal information as a whole, as it was being conducted at the time of the underlying investigation report, did not comply with PIPA.

The Commissioner suggested, however, that the system could be brought into compliance if it were aimed at only maintaining a list of banned customers. He therefore strongly encouraged those involved to work with the OIPC to find a solution for collecting personal information of a nature, and in a manner, that complies with PIPA. Subsequently, the system was modified to limit the amount of information collected and to purge the information of customers within twenty-four hours. The information of designated customers would be retained for one year, if the establishment determined them to be violent or otherwise undesirable for re-entry from a customer safety perspective. The Commissioner found that, with those modifications, the system was compliant with PIPA.

Limitations on Use of Personal Information (s. 14)

Order P09-02 — Shoal Point Strata Council

Several residents of a condominium governed by a Strata Council complained that it was gathering personal information through video surveillance cameras, contrary to section 14 of PIPA. During the investigation, the issue also arose as to whether Shoal Point was in compliance with section 10(1) of PIPA.

The Adjudicator found that section 14 of PIPA permits the use of video surveillance on exterior doors and in the parkade for the purposes of preventing unauthorized entry, theft or the threat to personal safety or damage to property, but not for bylaw enforcement. He

also found that it does not permit the use of video surveillance in the pool area or outside the fitness room. Nor was it appropriate to provide access to the video surveillance system to residential units through the television cable system or to conduct a routine review of the previous day's footage, in the absence of a complaint or evidence of unauthorized entry, theft or the threat to personal safety or damage to property. Finally, he found that the Strata Council failed to demonstrate compliance with the requirement to provide notice of collection of personal information in accordance with section 10(1) through the failure to provide details of the signs posted to notify individuals of video surveillance.

6.3 Judicial Reviews

Judicial reviews are reviews by the BC Supreme Court of an OIPC order or decision.

Custody or Control – Scope of FIPPA (s. 3); Information Rights (s. 4)

Order F08-01 — Simon Fraser University

This judicial review was the result of a petition by Simon Fraser University against Order F08-01, in which an Adjudicator found that records of a subsidiary company of SFU were under the control of SFU. The Order arose from a request from an individual for records in the possession of SFU's University Industry Liaison Office relating to SFU's spinoff companies. The Adjudicator found that the records were under the control of SFU because the records related to SFU's mandate; the records were received by an SFU employee in the course of their employment; and there were several reasons why spinoff companies and SFU should be treated as one entity.

The court found that the Adjudicator erred in piercing SFU's corporate veil without applying the proper legal standing. It also found that the spinoff company was subject to PIPA and that it was inappropriate to find that records of an organization should be subject to two statutes respecting privacy. This decision is subject to an appeal before the British Columbia Court of Appeal which has not yet been heard.

Order F09-06 — University of British Columbia

The public body petitioned for judicial review of this order. The Adjudicator had found that the public body had control of certain records in the hands of certain entities where, for example, that entity's shares were 100% controlled by UBC. However, the adjudicator ruled that UBC did not have control of records in the hands of other entities such as the University of British Columbia Foundation, which was a separate statutory creation. The order was partially set aside by consent order and remitted to the OIPC for a hearing.

Procedural Issues – Time Limit for Responding (s. 7); Appropriate Person (s. 54(b))

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

The Ministry of Labour and Citizens' Services and third party IBM sought judicial review of the Commissioner's decision directing the ministry to provide the applicant with a

complete response to the applicant's request. The ministry and IBM argued that IBM's request for a review of the ministry's decision to disclose information that IBM said was protected by section 21 of FIPPA freezes the ministry's duty under sections 7 and 8 to respond to the applicant's access request respecting other access exceptions. In a preliminary decision, the Commissioner determined this position was not tenable. The Commissioner also rejected the assertion that the access applicant was not an "appropriate person" to participate in the inquiry regarding the section 21 issue.

On judicial review, the Court found that, taking into account the modern principles of statutory interpretation and giving appropriate deference to the Commissioner in the interpretation of his home statute, the Commissioner's decision was both reasonable and correct.

Cindy Hamilton
REGISTRAR OF INQUIRIES

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

Order F08-22 — Fraser Health Authority

The third party Sodexo sought a judicial review of the Commissioner's order that the Fraser Health Authority 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.

The Commissioner concluded that section 17(1)(e) was not applicable because what was at issue in the case was pricing information in a concluded contract, the product of negotiation, not "information about negotiations carried out by or for a public body". The Commissioner also determined that the disputed information did not meet the "supplied" test in section 21(1)(b). For these reasons, the public body was ordered to provide access to the disputed information.

Prior to the matter being heard by the Court, Sodexo discontinued the judicial review proceeding.

Disclosure harmful to the business interests of a third party (s. 21)

Order F08-10 — The Board of Education of School District No. 69 (Qualicum)

The third-party unions and the public body petitioned for judicial review of the section 21 aspects of this order. The Senior Adjudicator had found that section 21 did not apply to five pages of information related to a grievance the unions had filed with the public body. The judicial review was resolved with consent orders setting aside the section 21 aspect of the order, without remittal to the OIPC.

6.4 Adjudication

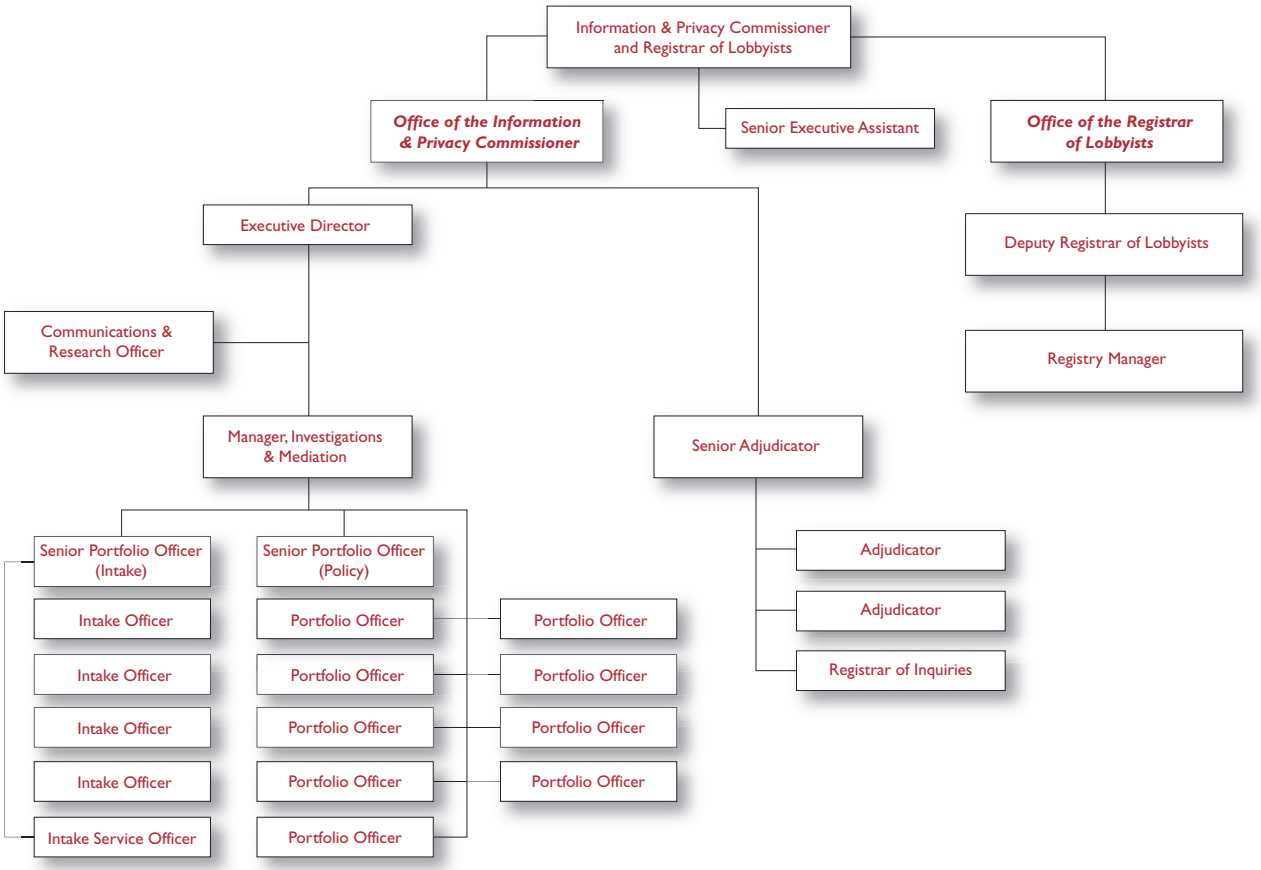
Adjudications are reviews by judges of OIPC decisions regarding access to information in the custody or control of the OIPC. Only one adjudication occurred during the past fiscal year.

Adjudication #22

An applicant requested copies of correspondence stored in an OIPC investigation file relating to his complaint against the Vancouver Police Department. He had complained that the VPD had improperly disclosed his personal information and was dissatisfied with the outcome of his complaint to the OIPC. The OIPC denied access to its complaint file in accordance with section 3(1)(c) of FIPPA, on the grounds that the records were the operational records of an officer of the Legislature.

A judge of the British Columbia Supreme Court, acting as an adjudicator under section 60 of FIPPA, confirmed the decision of the OIPC to deny the applicant access to the requested records under section 3(1)(c) of FIPPA.

7 ORGANIZATION CHART



8 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 2,900 public agencies, and accords access to information and protection of privacy rights to citizens. PIPA regulates the collection, use, 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 *Lobbyist 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 for 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 is 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):

	2010			2009
	OPERATING	CAPITAL	TOTAL	TOTAL
Appropriation	$3,822,000	$45,000	$3,603,000	$60,000
Other amounts (LRA funding)	$73,581	0	0	0
Total appropriation available	$3,895,581	$45,000	$3,603,000	$60,000
Total operating expenses	-$3,895,581	-	-$3,481,061	
Capital acquisitions	-	-$45,000	-	-$22,766
Unused appropriation	$0	$0	$121,939	$37,234

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 2009/10 fiscal year was $16,717.87. 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):

	2010			2009
	COST	ACCUMULATED AMORTIZATION	NET BOOK VALUE	NET BOOK VALUE
Computer Hardware and Software	$161,126	-$125,172	$35,954	$26,542
Furniture and Equipment	$36,172	-$10,950	$25,222	$11,873
Total	**$197,298**	**-$136,122**	**$61,176**	**$38,415**

6. Leasehold Commitments

The OIPC has a leasehold commitment with Accommodation and Real Estate Services for building occupancy costs and $211,272.55 was paid out in fiscal 2009/10. Payments for office space for the fiscal 2010/11 are estimated at $331,000.00.

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.