Office of the Information & Privacy Commissioner
FOR BRITISH COLUMBIA

ANNUAL REPORT

2004
2005

Library and Archives Canada Cataloguing in Publication Data
British Columbia. Office of the Information & Privacy Commissioner.
Annual report. – 2004/2005-

Annual Report year ends Mar. 31.
First report covers the period from Aug. 1, 1993 to Mar. 31, 1994.
Also issued in electronic format through the Internet.
ISSN 1198-5909 = Annual report – British Columbia.
Office of the Information & Privacy Commissioner.

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

KEB505.62 342.711'062 C94-960212-4
KF5753.I5B74

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

August 8, 2005

Bill Barisoff MLA
Speaker Designate
Legislative Assembly of British Columbia
Victoria BC

Dear Speaker Designate Barisoff:

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

This report covers the period from April 1, 2004 to March 31, 2005.

Yours sincerely,

David Loukidelis
Information and Privacy Commissioner
for British Columbia

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Third Floor, 756 Fort Street
Telephone: (250) 387-5629 Facsimile: (250) 387-1696
Toll Free enquiries through *Enquiry BC* at (800) 663-7867 or (604) 660-2421 (Vancouver)
website: http//www.oipc.bc.ca

Table of Contents

List of Tables

Commissioner's Message

It has been a privilege to spend the last six years promoting transparent and accountable government and privacy protection in both the public and private sectors and I am grateful for the opportunity to serve the citizens of this province.

Several of my colleagues have been with the office, which opened in 1993, since its earliest days. Others have joined more recently, in some cases after I took the job. All of my colleagues, regardless of when they started working in the office, have my respect and gratitude. Our office is, at present, only 17 strong yet we manage each year to handle one of the highest caseloads of any such office in Canada. This is possible only because my colleagues are hard-working, knowledgeable and efficient professionals. I have often thanked them publicly and privately for their efforts—and good humour—in serving the public and I thank each of them again one last time.

The 3,613 files we closed this year is a record for our office. By files I mean the broad range of activities in which we engage, including requests for review (access to information appeal mediations and adjudications), extensions of the time for response to access requests, approvals for indirect collection of personal information, applications to disregard access to information requests, privacy breach notifications, privacy complaints, access requests to our office as a public body under the legislation, reviews of proposed legislation, policy consultations by public bodies, privacy impact assessment reviews, requests for information about the legislation and other matters, speaking engagements and media interviews.

Despite our best efforts, however, our ability to do our job in a timely and professional fashion continues to face considerable challenges. This fiscal year we received additional funding for our oversight responsibilities under British Columbia's private sector privacy law, the *Personal Information Protection Act* (PIPA). But the cuts to the budget for our public sector oversight duties continue to negatively affect our ability to provide effective and timely oversight. This year we have experienced the first noticeable backlog of files, measured by the number of files opened during the year minus the number of files closed during the year. We received a total of 1,266 requests for review and complaints and closed 1,077, leaving a backlog of 189. This is more than three times the backlog that existed at the end of the previous fiscal year and represents the annual workload of two full time Portfolio Officers, who are responsible for mediating access and privacy complaints.

An effective access and privacy law requires effective oversight of compliance, which in turn depends on adequate funding for the oversight agency. The Legislative Assembly's Select Standing Committee

on Finance and Government Services recommended the three-year 35% cut to our public sector oversight resources. The Committee has more than once indicated that added resources will be recommended where need is shown. This was the case with the added funding we received for our PIPA responsibilities, which began at the start of 2004.

When I asked the Select Standing Committee on Finance and Government Services for added funding for our new PIPA responsibilities, I said we hoped the request would cover the added workload without impeding our existing *Freedom of Information and Protection of Privacy Act* (FIPPA) responsibilities. I added that, if this were not so, the OIPC would seek further resources to allow us to serve the public well.

In light of the significant case backlog we now have, and the increasing delays involved in our doing our work, I am concerned that we are not properly discharging our duties to the public and that the OIPC needs more resources to deal with increased workloads and to ensure we provide the timely and diligent oversight the public has a right to expect of us. This is a message that I expect will be carried forward to the Committee during this autumn's round of budget deliberations.

I am also concerned that a shortage of resources for provincial government ministries for responding to access to information requests is impeding the public's right of access to information. This is not the first time my annual report message has raised the issue of delay in public body responses to access requests—my first message, in 1999-2000, devoted an entire section to the problem. Delay in response to access requests has come up in later annual reports, and I have expressed concern about it in other venues.

This year, we received 28% more complaints about the timeliness of responses by public bodies to access requests than ever before. I firmly believe that it is time for provincial government ministries to invest more, not less, money in their access and privacy offices so the public's right to know is not impeded by delay. In the past, our office has helped struggling ministries to meet their statutory access to information obligations. We continue to be willing to do this—our own resources permitting—but one wonders whether more forceful action is necessary where delays are chronic.

This does not reflect poorly on individual information and privacy employees in provincial government ministries. Time and again I have been impressed by the professionalism and dedication they display in approaching their statutory duties under the *Freedom of Information and Protection of Privacy Act*. The same goes for the access and privacy staff of the more than 2,000 other public bodies in the province—Crown corporations, self-governing professions, local governments, police departments, universities, colleges, schools and health authorities—who

breathe life every day into the access and privacy rights of all British Columbians. I have valued all of their efforts over the years and thank them again for their service to the public.

Rolling Out Private Sector Privacy

As I said in my last annual report message, the arrival of private sector privacy in British Columbia at the start of 2004 was a major development. With the introduction of the *Personal Information Protection Act* (PIPA), British Columbia joined other Canadian jurisdictions in extending internationally recognized privacy principles to the broad private sector. Our experience over the last year in overseeing PIPA confirms my view that PIPA strikes the proper balance between the privacy rights of individuals and the need of organizations to collect, use and disclose personal information for their activities.

Before PIPA came into force, my office invested considerable time in preparing resources to support organizations and individuals dealing with PIPA. This work continues. During the last year, we conducted an extensive, broad consultation with stakeholders on our draft discussion paper, which addressed selected employment privacy issues. We have carefully considered the feedback we got from employers, employer groups, unions, labour organizations and advocacy groups and will soon circulate a further draft for consultation.

On the topic of support materials, during the year we published new resources on our website dealing with use of social insurance numbers, identity theft, faxing or emailing of personal information, security tips for working with personal information outside the office, tips for organizations in responding to privacy complaints and tips for individuals in making complaints to organizations. We also revised our comprehensive guide to PIPA for organizations.

As 2004 moved into 2005, requests by organizations and individuals for information or assistance continued to increase significantly, reflecting, I believe, growing awareness of PIPA and its requirements. We also saw an increase in the pace and number of formal complaints. I have no doubt, however, that the numbers of complaints would have been higher were it not for our policy of referring would-be complainants back to the responsible organizations to attempt a private resolution of the matter before complaining formally to us. As we move ahead, I have every expectation that our PIPA workload will continue to increase and that new and interesting issues will confront us.

We will be assisted in meeting those challenges by ongoing close collaboration with our colleagues in the Office of the Information and Privacy Commissioner of Alberta and the Office of the Privacy Commissioner of Canada. Our regular contact with them helps us keep

abreast of, and contribute to, emerging good practice in overseeing private sector privacy legislation.

Time for Improvements to Our Information and Privacy Law

It has often been said, with good reason, that a well-crafted freedom of information law is indispensable to the proper functioning of a healthy democracy, while balanced, meaningful privacy rights are important in protecting individuals from the state's power. FIPPA has, for over a decade, served the vital function of guaranteeing the public access to information and protecting personal privacy. It is a primary mechanism by which public agencies are held accountable to the citizenry. All laws must, however, be reviewed and amended over time to ensure that they keep pace with the ever-changing social and political landscape. This is no less true with FIPPA than any other legislation.

This is why FIPPA is reviewed periodically by an all-party Special Committee of the Legislature, whose task is to review the legislation and recommend amendments to ensure that the public's access to information and privacy rights remain vigorous and meaningful.

Most recently, in May of 2004 the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* released its excellent report, *Enhancing the Province's Public Sector Access and Privacy Law*. The Special Committee recommended 28 changes to the Act to ensure that the access and privacy rights of British Columbians remain current and effective.

The most important access to information recommendation relates to s. 13, which gives public bodies the discretion to refuse to disclose "advice or recommendations developed by or for a public body or a minister." This section was never intended to shield factual information,[1] but a 2003 decision by our Court of Appeal gave a sweeping and, in my view, excessively broad interpretation to "advice" under s. 13. This decision threatens to seriously erode the public's right of access to information in order to hold public bodies accountable, a goal explicitly stated in s. 2 of the legislation. It could also allow a public body to refuse to disclose to individuals their own previously available personal information. The Special Committee considered this decision and laudably and sensibly recommended that s. 13 be amended to ensure that accountability through FIPPA is not impaired and I urge the government to do so as soon as possible.

The Special Committee also recommended a number of changes designed to promote a culture of openness and enhance accountability in cost-effective ways. It recommended that public bodies be required to adopt schemes for the routine disclosure of records. It also

1 This is made plain by s. 13(2)(a), which prevents a public body from withholding "factual material".

recommended that public bodies make routinely available, free of charge and without an access request, the personal information of anyone who requests it, subject of course to any access exceptions that might apply.

I have been saying for many years that routine, pro-active disclosure of information has many advantages over a reactive, request-triggered approach to freedom of information. Routine disclosure is expeditious, consistent with the goals of openness and accountability and less expensive.

The identity of a requester and the motives behind an access request are irrelevant considerations in granting access to public records. The Special Committee recommended a legal right to anonymity for anyone making an access request, other than those requesting access to personal information. I strongly support this commendable approach.

Last, the Special Committee recommended a series of changes to improve the oversight powers of my office and create simpler and more efficient processes for us to resolve access and privacy disputes. In a spirit of moving away from process-driven to results-focussed oversight, the Special Committee recommended that the complaint, review and inquiry processes be combined into one unified, less confusing appeal process. Another important recommendation would explicitly allow my office to require applicants to attempt to resolve their disputes with public bodies in a manner that we direct. Last, the Special Committee made a series of recommendations designed to improve the Commissioner's powers to enforce orders, order production of records and compel statistical information from public bodies.

The government's intentions with respect to fully implementing the recommendations of the all-party Special Committee are not known. The government has an excellent opportunity here to further improve FIPPA on the basis of the bi-partisan recommendations of the Special Committee and I urge it to seize the opportunity quickly. British Columbia's law is often said to be the best access and privacy law in Canada and there is a lot to that claim. The opportunity is here to make it even better.

Privacy and the Outsourcing of Personal Information Management

We live in an increasingly seamless world, one in which our personal information flits across and between continents every day in the ordinary course of business. At the same time, the tasks undertaken by government have grown increasingly complex and efficient management of information is ever more essential. Governments have increasingly been following the lead of businesses in contracting out services formerly done in house. This includes the outsourcing of data

management services, including data storage and processing, and some of these outsourcing arrangements may involve trans-national transfers of personal information.

Concerns arose early last year about risks to personal information involved in the outsourcing of services. The provincial government announced early in 2004 that it intended to outsource administration and operation of British Columbia's public health insurance scheme to a company located in BC but owned by a US-linked corporation. Soon after the announcement, a lawsuit was launched alleging that outsourcing to a US-linked service provider unlawfully exposed the health information of BC residents to access under the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act)*.

Almost immediately my office began receiving requests from the government itself, media in Canada and elsewhere, interest groups and members of the public for guidance about possible *USA Patriot Act* privacy implications where personal information is part of an outsourcing arrangement and a service provider with US links is involved. We also received a formal complaint about the proposed health insurance plan outsourcing.

The level of public concern and the requests for guidance were such that I decided to assess, on a consultative basis, the implications of the *USA Patriot Act* for privacy compliance under FIPPA. We conducted a national and international public consultative process to provide general guidance and recommendations on two questions relating to the *USA Patriot Act* and outsourcing of public services. First, we asked whether the *USA Patriot Act* would permit US authorities to access the personal information of British Columbians that is in the control of a service provider with US links. Second, we asked, if US law permits such access, what are the implications for public body compliance with the personal privacy protections in FIPPA and what measures can be taken to mitigate these risks? My goal in examining these questions was to assess *USA Patriot Act* privacy implications and to recommend practical and effective measures to meet any risks we identified.

I invited submissions on these two questions and in response received more than 500 submissions from across Canada, the US and Europe. We heard from individuals, governments both domestic and foreign, labour groups, information technology companies and associations, health care providers, library associations, privacy advocacy organizations and privacy commissioners. We also heard from the FBI and the Department of Homeland Security.

Many of the submissions we received addressed the two questions about *USA Patriot Act* implications, but a great number of them raised far broader issues. A number of themes ran throughout the submissions, three of which merit mention here.

First, many people fear they are losing control over what happens to their personal information and worry that their privacy rights are being displaced by economic and national security priorities.

Second, many people believe that information technology developments are fuelling the appetites of governments for larger data banks and for the mining of personal information for national security and other purposes. They fear that new laws since September 11, 2001, have encouraged or compelled the private sector to share personal information with government authorities for national security or law enforcement purposes. They also fear diminished accountability and transparency of the actions of law enforcement agencies in this regard.

Third, there are indications of a trend developing whereby personal information collected for national security purposes may be used more and more for ordinary law enforcement purposes. Such a trend blurs the traditional division between the state's role in protecting the public from domestic and foreign national security threats and its role in enforcing ordinary criminal and regulatory laws, a blurring of roles that could have significant implications for privacy.

Having reviewed the submissions, we quickly realized that our two questions could not be isolated from broader and inter-related themes such as those I have just mentioned. All of these themes underscore privacy's importance, point to expanding risks for privacy in a more and more interconnected world and highlight the risks and potential impact of disclosure of personal information abroad, notably to foreign authorities, without there necessarily being any meaningful privacy protection after disclosure abroad. To a significant extent, therefore, the report we produced last October examines wider questions arising out of these themes and offers recommendations to address them.

Our report's recommendations, based on careful consideration of the hundreds of thoughtful submissions and our detailed analysis of plausible legal and policy options, were designed to provide meaningful yet reasonable solutions. Our report is, however, only part of a dialogue that will continue for years, including through the follow-up report we will issue later this year or early next year on government's progress with our recommendations.

Blurring the Lines—National Security and Law Enforcement

As our *USA Patriot Act* work revealed, there is a growing, and disturbing, trend towards increased blurring of the longstanding boundaries between national security activities and ordinary law enforcement. National security measures refer to steps taken by states to ensure their

survival against perceived external or internal threats. Law enforcement more broadly describes enforcement measures to ensure compliance with statutes.

The risk of terrorist attacks on Canada cannot be discounted—the attacks last year in Madrid and this year in London are stark reminders of the real, ongoing threat from international terrorism. Measures are needed to help prevent them and to allow us to do our part in fighting terrorism internationally. While extraordinary powers are often necessary to protect national security, such powers must be clearly linked to the objectives they are created to achieve, must be no more extensive than absolutely necessary and must be subject to meaningful, independent oversight to ensure they are not abused (including by being applied to activities that have nothing to do with terrorism).

Government must, therefore, take great pains not to overstep the line in equipping itself to discharge its duties. Although it may be true that the more freedom people have the greater the potential risks, the corollary is equally important. Every increase in security almost inevitably curtails rights and freedoms that are at the heart of democratic societies. This means care and deliberation, not haste and panic, must guide legislators and those who enforce our laws.

The Canadian *Anti-Terrorism Act* is under review by the House of Commons Subcommittee on Public Safety and National Security. My submission earlier this year to the Committee made two key points.

First, it is vital that Canada's national security needs not blur any further into ordinary law enforcement interests and demands. The constitutional and statutory privacy protections we enjoy should not be set adrift in the name of national security to founder on the rocks of law enforcement expedience. This has already occurred in Canada to a notable degree. To give only one example, airlines now can be compelled, without a warrant, to provide air passenger information to police for anti-terrorism purposes, but that same information can be used for certain ordinary law enforcement purposes.

Second, there is a pressing need for meaningful, independent oversight of surveillance activities to ensure that public safety interests are carefully balanced against individual rights to privacy. Independent oversight is one of the basic characteristics distinguishing free societies from their totalitarian counterparts. Oversight cannot stop mistakes from occurring, to be sure, but it can at least set reasonable limits on the circumstances and manner in which surveillance is conducted and expose mistakes and intentional wrongdoing to the light of day.

Information Management and Records-Creation Legislation

A cornerstone of accountable government is good information management. The effectiveness of the public's right of access to information depends on sound information management. If governments are to be held accountable and the public are to have meaningful rights of access to government information, information must be accurately and securely preserved to ensure there is a record of what has been done. Without reliable recorded evidence, governments cannot demonstrate that they have used public resources responsibly and have discharged their duties and used their powers lawfully. If there is no effective information management—the systematic control, organization, access to and protection of recorded information through its creation, use, permanent retention or destruction—the public's right of access to information and its ability to hold public institutions accountable will be seriously threatened.

Traditional records management theory focuses on a subset of information that can be described as business records. FIPPA extends the challenge of traditional records management to the entirety of paper, audio, visual and electronic information in the custody and control of any public body, from an obscure inter-office memo to a Cabinet submission.

Traditional records management is also challenged by the expanding reliance on electronic records and databases. The sheer volume, and variety, of electronic records makes it difficult to catalogue, organize and preserve them in a way that keeps them accessible. These problems are exacerbated as hardware, software and storage media become obsolete, leaving behind records that can no longer be read, making a once-valuable government asset worthless.

There are other challenges. For example, the coming sea-change in our public service—the demographics that will see massive retirement numbers in the coming decades are only one driver of change in the public service—makes modern information management all the more critical to government. The corporate memory of governments is aging and much of it will soon be gone. As another example, the move towards function-based, cross-boundary government, which has many attractions, makes information management both complex and crucial across old and new boundaries and within and between functions.

We therefore need information management laws and standards that are designed to maximize, among other things, completeness, accuracy, integrity and preservation of information and timely access to information within and from outside government. These objectives are desirable to foster quality in governance and to promote accountability through access to information.

A shortcoming of traditional records management rules is that they apply only after a record has been created. Many US states have laws that prescribe the types of decisions, actions or deliberations of government that must be documented. In British Columbia, some statutes require certain actions or decisions to be documented, but any legal obligation for ministers or civil servants to create and maintain full and accurate records is weak, if not non-existent. There is no overarching legal duty to document government actions or decisions.

A modern information management framework should include, therefore, a requirement that officials record specified kinds of decisions and actions, with this duty to create records being supplemented by government-wide, consistently applied information management rules and standards. Further, an adaptable, scaleable, government-wide information architecture and e-record directories are necessary. An accountability framework for information management within each institution, with a coordinated central command structure for oversight and accountability within and across departments, is also desirable.

Individual civil servants should, as well, be responsible for information management tasks within their own employment duties, with relevant requirements being made a condition of employment and of employee appraisal. Information management should form part of executive level compensation assessment and information management performance should be an institutional performance standard and subject to regular appraisal.

I have spoken on a number of occasions over the last six years about the need to ensure the provincial government has modern, comprehensive information management systems in place. For many this is not a top of list issue, I know, but, as mundane or even arcane as it may seem, it is of critical importance. I therefore urge the government to assess the situation and ensure that its information management framework meets the challenges discussed above.

These are only some of the issues and challenges to cross my desk this year. There have been many more, and many others will face our office in the years to come.

David Loukidelis
Information and Privacy Commissioner for British Columbia

Victoria BC
August 2005

Role and Mandate of the Office of the Information and Privacy Commissioner

The Office of the Information and Privacy Commissioner (OIPC) was established in 1993 to provide independent review of access to information decisions made by public bodies under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

FIPPA gives citizens a right of access to records held by more than 2,000 public agencies, including provincial government ministries, Crown corporations, local governments, school boards, colleges, universities, municipal police forces, hospitals, health authorities and self-governing professions. FIPPA creates a set of rules by which public bodies must abide when responding to a request for records. Those rules include timelines within which public bodies must respond to an access request and the circumstances in which public bodies may withhold information.

FIPPA also restricts the collection, use and disclosure of personal information by public bodies. The OIPC investigates complaints that public bodies have failed to comply with these privacy protection provisions.

The Information and Privacy Commissioner is also responsible for overseeing compliance by private sector organizations with the *Personal Information Protection Act* (PIPA). That Act, which covers more than 300,000 organizations—including businesses, charities, associations, trade unions and trusts—contains rules about organizations' collection, use and disclosure of individuals' personal information.

The Commissioner is generally responsible for monitoring how the two Acts are administered to ensure that their purposes are achieved. Under FIPPA, the Commissioner has the power to:

- Investigate, mediate and resolve appeals concerning access to information disputes, including issuing binding orders
- Investigate and resolve privacy complaints
- Conduct research into anything affecting access and privacy rights
- Comment on the access and privacy implications of proposed legislation, programs or policies
- Comment on the privacy implications of new technologies and/or data matching schemes
- Educate the public about their access and privacy rights.

Under *PIPA,* the Commissioner is empowered to:

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

While the Commissioner is responsible for promoting and enforcing open and accountable government through access to information and privacy compliance, he is accountable to the public and the Legislature in a number of ways, including these:

- The Supreme Court of British Columbia can judicially review the decisions of the Commissioner
- The administrative records of the Commissioner's office are subject to FIPPA
- A complaint can be made to the Speaker of the Legislative Assembly about the Commissioner or the OIPC
- The Commissioner must comply with the *Public Service Act* in hiring, managing and terminating staff
- The OIPC's annual budget is set based on recommendations by an all-party Select Standing Committee of the Legislative Assembly, and the Standing Committee reviews the OIPC's budget and service plans
- The Commissioner publishes an annual report, outlining all of the major activities of the office and providing a financial report.

The Commissioner has the statutory power to delegate some of his responsibilities for investigating and resolving access and privacy appeals. The Commissioner has delegated the authority to his staff to investigate appeals and complaints, hold inquiries, provide policy advice, comment on anything affecting access and privacy rights and deliver educational seminars.

A Snapshot of OIPC Files Received and Closed Last Year

Table 1.
Total OIPC Files Received and Closed, 1 April 2004-31 March 05

File Type	Files Received	Files Closed [2]
Application to Disregard	2	4
Breach Notification	3	3
Complaint	564	433
Freedom of Information Request	22	23
Investigation	6	6
Legislative Review	68	75
Media	96	97
Meetings	41	31
No Reviewable Issue	30	30
Non Jurisdictional Issue	14	22
Policy or Issue Consultation	136	127
Privacy Impact Assessments	7	7
Special Projects	34	27
Public Interest Notification	25	25
Reconsideration	1	1
Request for Time Extensions (all types)	115	115
Request for Information	1648	1761
Request for Review	702	644
Research Agreement	1	1
Speaking Engagements	51	40
Read & File	125	130
Internal Review	12	11
Total	**3703**	**3613**

2 Some files closed in fiscal 2004-2005 were received in fiscal 2003-2004.

Access to Government Information

British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA) came into force on October 4, 1993. Politicians from both the left and right of the political spectrum had introduced 12 different access and privacy bills in the Legislative Assembly during the preceding seventeen years, but none had survived Bill 50, which became FIPPA.

All Canadian provinces and territories now have access and privacy laws, with Nova Scotia being first off the mark in Canada in 1977. Federally, the *Access to Information Act* and *Privacy Act* came into force in 1983. South of the border, the United States federal *Freedom of Information Act* was passed in 1966.

More than 46 countries around the world now have freedom of information laws. They span several centuries, with Sweden enacting its first access to information law in 1766. Elsewhere in Europe, Finland enacted a freedom of information law in 1951 and Ireland did so recently. Scotland has an access to information law and the *Freedom of Information Act* came into force in England and Wales earlier this year. A number of German states have access laws and new members of the European Union—notably those formerly in the Soviet bloc—have enacted access to information laws or are actively considering doing so.

It is a central tenet of democracy that public institutions are accountable to the citizens they serve, and accountability cannot survive in the absence of transparency. Freedom of information laws provide the legislative direction to ensure a healthy transparency in government operations. As s. 2(1) of FIPPA says, one of the purposes of the Act is to "make public bodies more accountable to the public … by giving the public a right of access to records".

The central importance of freedom of information for good government has been confirmed on many occasions, as the following passage from the Supreme Court of Canada decision in *Dagg v . Canada*[3] illustrates:

> As society has become more complex, governments have developed increasingly elaborate bureaucratic structures to deal with social problems. The more governmental power becomes diffused through administrative agencies, however, the less traditional forms of political accountability, such as elections and the principle of ministerial responsibility, are able to ensure that citizens retain effective control over those that govern them….
>
> The overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to

3 *Dagg v. Canada (Minister of Finance)* [1997] 2 S.C.R. 403

> ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry….

This is how the political philosopher John Plamenatz put it [4]:

> Access laws operate on the premise that politically relevant information should be distributed as widely as reasonably possible, and that the same information that is available to politicians and civil servants is also available to the ordinary citizens. In an open and accountable society, "[n]o leader or persuader possesses more than a small part of the information that must be available to the community if government is to be effective and responsible; and the same is true of the ordinary citizen."

Here in British Columbia, a 1991 law reform report by the BC Freedom of Information and Privacy Association put it this way:

> Information about how government decisions have been made, and why, must also be available on the ground of political accountability. Taxpayers pay for government and the information held by it. Many government agencies, and most individuals and interest groups, welcome a degree of public participation in decision-making. But meaningful and efficient participation depends also on access to relevant information held by government in its broad sense... .
>
> Access to information will gradually enhance the credibility of government with the public. It will justify public trust and the perception of government integrity and accountability. The public will perceive government decision-makers as administering in a fair and open manner. [5]

Access legislation is one mechanism by which governments and public institutions are held accountable. Others include fair elections, freedom of the press, freedom of speech and assembly, independent audit and oversight, the committee system in Parliament and the Legislature, *Hansard* and question period in the Legislature. As federal Information Commissioner John Reid has said, these other accountability mechanisms have little if any viability without the oxygen of information about what public institutions think, decide and do, about what governments know about their citizens, and about the costs and impact of decisions and actions.

Privacy Protection

In his book *Big Brother*[6], Simon Davies, an internationally known privacy expert, wrote:

> People who have no rights of privacy are vulnerable to limitless intrusions by governments, corporations, or anyone else who

4 John Plamenatz, *Democracy and Illusion* (London: Longman, 1973).
5 BC Freedom of Information & Privacy Association, *Information Rights for British Columbia* (FIPA, Vancouver: 1991).
6 Simon Davies, *Big Brother: Britain's Web of Surveillance & the New Technological Order* (London: Pan, 1996).

> chooses to interfere in your personal affairs. Imagine a world where government had an unfettered right to demand information from you, or to remove money from your bank account, or even to enter your house. The tragic history of many of the world's countries shows us that a nation denied the right of privacy is invariably denied all other freedoms and rights.

The term "privacy" is not actually defined in British Columbia's F*reedom of Information and Protection of Privacy Act,* and privacy can mean different things to different people. To some, privacy means the "right to be let alone". To others, it means anonymity. Still others believe it means the right to be unobserved. Under the Act, privacy means maximizing, wherever possible and to the extent that is reasonable, a citizen's control over the collection, use and disclosure of his or her personal information.

In order to receive public goods and services, citizens must provide a certain amount of personal information to the government. The scope and sensitivity of the personal information that must be produced in exchange for the service varies, depending on the service. For example, you will be required to disclose educational and income information if you are seeking a loan for university education; family status and income information if you require subsidized medication; eyesight, height and weight information if you require a driver's licence; and your name and home address if you require a building permit.

FIPPA is essentially a privacy roadmap. It contains a set of internationally recognized rules—called "fair information practices"—that govern the collection, use and disclosure of personal information by public bodies. Collectively, those rules reinforce the basic premise that public bodies must be appropriately restrained, transparent and vigilant in the management of personal information collected or compiled in the delivery of public services. FIPPA, therefore, deals with what the Supreme Court of Canada has called "informational privacy":[7]

> …[T]here is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the [Federal Task Force] put it: "[The] notion of [informational] privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which, it is divulged must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained; see, for example, the [federal] *Privacy Act*.

7 *R. v. Dyment*, [1988] 2 S.C.R. 417, at pp. 429-430

Modern privacy legislation emerged in the late 1960s when the Council of Europe began studying the effect of computer technology on personal privacy. The first European data protection law was enacted in Sweden in 1973, followed by West Germany and France. In 1980, the Organization for Economic Co-operation and Development (OECD) developed its *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, commonly referred to as the OECD Guidelines. In 1995, the European Union passed a Directive on data protection, a legal instrument that binds all member states. Among other things, the EU Directive prohibits the electronic export of personal data to any country that does not have an adequate level of legal privacy protections.

In North America, the *Fair Credit Reporting Act* was the first privacy-related law passed in the United States, in the late 1960s. Over the years, a number of industry-specific privacy laws have been enacted in the US. Three examples of the many US privacy-related laws now in place at the federal level alone are the health privacy rules under the federal *Health Insurance Portability and Accountability Act*, the financial privacy requirements of the Gramm-Leach-Bliley Act and privacy protection for children using the Internet, found in the *Children's Online Privacy Protection Act*.

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

Private sector privacy laws first emerged in Canada with Quebec's enactment in 1994 of privacy rules for the private sector. Then Parliament enacted the *Personal Information Protection and Electronic Documents Act*, which came into force in stages, beginning in 2001. British Columbia later enacted substantially similar legislation in the form of the *Personal Information Protection Act,* which came into force in 2004. (Our work under our private sector privacy law is discussed in part 6 of this report.)

Protection of Access & Privacy Rights through BC's FIPPA

A central purpose of FIPPA is to make public bodies accountable to the public by giving the public a right of access to records and limiting the circumstances in which access to records is refused. Another core objective of the law is to protect the privacy of citizens by specifying rules around the collection, use and disclosure of personal information by government.

To accomplish these important objectives, FIPPA:

- Establishes a set of rules specifying limited exceptions to the rights of access
- Requires public bodies to make every reasonable effort to assist applicants and to respond to access requests openly, accurately and without delay
- Requires public bodies to respond to access requests within legislated timeframes
- Requires a public body to account for information it withholds in response to a request for records
- Establishes strict standards around when and how public bodies may collect, use and disclose personal information
- Provides for independent review and oversight of decisions and practices of public bodies concerning privacy and access rights.

Who Is Covered by FIPPA?

FIPPA applies to more than 2,000 public bodies, including

- All ministries of the provincial government
- Crown corporations such as ICBC and BC Hydro
- Agencies, boards and commissions
- Local public bodies, which includes all municipalities and regional districts, universities, colleges and schools, health authorities, health boards and hospitals, and municipal police forces
- Self-governing professional bodies (such as the Law Society and the College of Physicians and Surgeons).

FIPPA applies only to "records", i.e., information recorded in some physical medium (including paper and computerized records).

Any person who wants access to a record must make a written request to the public body the requester thinks has the relevant records. It is not necessary to give reasons for or justify an access request. A person's motive for asking for a record is irrelevant in determining the right to obtain access to a particular record.

FIPPA places a positive duty on public bodies to respond openly, accurately and completely to requests for records. They must also respond without delay. This duty helps create a more open and transparent system and minimizes the possibility of delays.

Since there is often a lot of truth in the saying "access delayed is access denied", FIPPA imposes a time limit of 30 business days on public bodies to respond to requests and allows them to extend that time limit only in specified circumstances.

Public bodies may charge specified fees for access to records, but fees should not pose a barrier to access. Public bodies cannot charge individuals for access to their own personal information. Applicants can request fee waivers because of inability to pay or where the records relate to a matter of public interest.

In British Columbia, most access requests are made by individuals who are requesting their own information––over 65% of requests for review to the Office of the Information and Privacy Commissioner are made by such individuals.

In responding to requests for information, public bodies must provide applicants with written decisions and, where they decide to deny access, must give specific reasons for doing so. Exceptions to the right of access are limited and are designed to protect certain important public and private interests, including:

- Personal privacy
- Third-party business interests
- Solicitor-client privilege
- Law enforcement interests
- Inter-governmental relations
- Economic and financial interests of the public body
- Personal and public safety.

The Importance of Independent Oversight

One of the most important features of FIPPA is the right of citizens to appeal or complain to an independent agency—the OIPC—about any refusal to disclose information or any action or decision by a public body concerning personal privacy. Independent scrutiny helps ensure that government actions and decisions with respect to access or privacy are made in accordance with rules set out in law and not on the basis of the self-interest of the bureaucracy or the government of the day.

Anyone who is dissatisfied with a public body's response to his or her access request can ask the Commissioner to review the response. This includes any decision to withhold or sever information, correct personal information, adequately search for responsive records, charge a fee or refuse to waive a fee. The OIPC will look into the matter, which will be resolved by mediation or by formal inquiry and order. The OIPC's processes for resolving matters are completely independent of government and impartial.

Table 2 describes how requests for review were resolved last year.

Type	Disposition							
	Mediated	No Reviewable Issue	Non Jurisdictional	Referred Back to Public Body	Withdrawn	Notice of Inquiry Issued	Order Issued	Total
Deemed Refusal	97	12	0	1	3	10	4	**127**
Deny Access	88	3	0	2	2	10	5	**110**
Partial Access	236	5	1	10	26	18	19	**315**
Fees	13	0	0	1	0	0	5	**19**
Notwithstanding (s.79)	2	0	1	0	0	0	0	**3**
Refusal to Confirm or Deny	1	0	0	0	0	0	1	**2**
Scope	2	0	0	0	0	0	3	**5**
Third Party	8	1	0	0	0	0	3	**12**
Transfer	0	0	0	1	0	0	0	**1**
Total	**447**	**21**	**2**	**15**	**31**	**38**	**40**	**594**

8 Some of these files may have been received in fiscal 2003-2004. This figure includes files closed by order.

Table 3. Disposition of FIPPA Requests for Review, by Public Body

Table 3 shows the disposition grounds for requests for review by public body.

Public Body	Disposition: Mediated	No Reviewable Issue	Non Jurisdictional	Referred Back to Public Body	Withdrawn	Notice of Inquiry Issued	Order Issued	Total
Insurance Corporation of BC	120	0	0	3	7	2	1	**133**
Vancouver Police Department	27	0	0	0	3	0	1	**31**
Ministry of Health Services	12	2	0	1	0	1	1	**17**
Provincial Health Services Authority	11	0	0	0	0	2	4	**17**
Ministry of Public Safety and Solicitor General	10	0	0	0	1	2	3	**16**
Ministry of Attorney General	10	1	0	0	0	2	2	**15**
Ministry of Children and Family Development	8	0	0	1	1	1	2	**13**
Interior Health Authority	11	0	1	0	0	0	0	**12**
Vancouver Coastal Health Authority	7	0	1	0	0	2	0	**10**
Ministry of Human Resources	9	0	0	0	0	0	0	**9**
Vancouver Island Health Authority	9	0	0	0	0	0	0	**9**
All Other Public Bodies	213	18	0	10	19	26	26	**312**
Total	**447**	**21**	**2**	**15**	**31**	**38**	**40**	**594**

Who Is Making Access Requests?

British Columbians take full advantage of their rights to access under FIPPA. In calendar year 2004, approximately 10,500 requests for information were made under the Act to government ministries alone, and 80% of those requests were from individual citizens. [9] (This notable number of requests does not include requests made to BC's many other public bodies, including Crown corporations, local governments, school boards, colleges, universities, health authorities or self-governing professions.)

9 Ministry of Management Services

Consistent with previous years, almost 80% of the access appeals filed with our office were from individuals. This is not surprising, since the access process is a key mechanism for individuals who want to know what personal information government has about them or want to get copies of their own personal information from government.

As for accountability to the public, requests by the media were up 6% of the total number of access appeals filed. The remaining 14% of access appeals to our office came from a wide variety of organizations and groups.

Resolving Disputes Through Mediation

If a dispute concerns a public body's decision to sever or withhold information, FIPPA refers to the matter as a "review". An applicant wishing to request a review must do so within 30 business days after receiving a public body's response to the access request and must include a copy of the original response and the public body's written decision.

Section 55 of FIPPA allows the Commissioner to authorize mediation for any matter under review. It is the normal practice for the OIPC to refer a review to a Portfolio Officer, who will try to resolve the matter through mediation. In this process, the Portfolio Officer is not an advocate for either side. Mediation fosters ongoing dialogue between the requester and the public body and is less expensive, less onerous and more expedient than a formal inquiry.

In attempting to mediate reviews, the Portfolio Officer ensures the applicant has received all of the information he or she is entitled to receive. This typically involves discussing the issue with all parties, reviewing the records in dispute, examining the legislation, considering previous relevant decisions by the OIPC, other commissioners and the courts, and attempting to generate mutually acceptable options for resolution of the matter. FIPPA allows 90 business days to resolve a review. If the matter cannot be resolved during this time period, the matter may proceed to a formal inquiry before the Commissioner or his delegate.

Mediation of reviews may result in a number of outcomes, including the following:

- More information is released
- The issues in dispute are narrowed
- The public body's decision is further clarified
- The applicant's initial request is further clarified
- The matter is referred to another agency for resolution
- An applicant's questions or concerns underlying the request are addressed.

Case Summaries: FIPPA Requests for Review

The following selection of some successfully mediated requests for review illustrates typical access to information disputes that we resolve each year. We also hope they are instructive for those using the *Freedom of Information and Protection of Privacy Act*.

Preparing a Cabinet Minister for a TV Interview

A municipality disagreed with a ministry over the right approach to the construction of a highway upgrade. After the ministry announced its plans, the municipality's lawyer asked for copies of all records related to the upgrade project, including internal emails, environmental data, land acquisition reports, engineering reports, costing data and polling data.

The lawyer got most of what he wanted. What he didn't get—and the reason he came to us with a request for review—was an email from the Public Affairs Bureau to ministry communications staff providing tips on how the minister should respond to anticipated questions in a TV interview. As the highway project was controversial and had a high political profile, the government wanted to be sure that questions about its strategy for dealing with the municipality were handled with great care.

Section 13(1) of FIPPA provides that the head of a public body may refuse to disclose to an applicant information that would reveal advice or recommendations developed by or for a public body or a minister. However, s. 13(2) provides that the head of a public body may not refuse to disclose any factual material.

In this case, we suggested that the ministry release most of the contents of the email as being statements of fact or material that was already publicly known. The TV crew had made its questions publicly known in advance, and some of the proposed answers suggested to the minister in the email were simply statements of fact or had already been aired. We agreed that it was reasonable to sever advice on how to deal with questions the answers to which were a matter of interpretation rather than fact and had not already been publicly stated by the minister.

The ministry reconsidered its decision and released the information in accordance with our suggestions.

Records Relating to the Death of a Resident of a Mental Health Facility

Following the death of a resident of a mental health facility, a reporter asked for a copy of the internal review or investigation into the death as well as any other documents discussing the death.

The health authority denied access to two records, the liability reporting form (citing the ss. 15 and 22 FIPPA exemptions) and the second a critical incident review (citing s. 51 of the *Evidence Act*).

During mediation, the health authority disclosed part of the first record, severing the deceased resident's medical information.

The remaining record had been created as a result of a request by the Chief of Psychiatry for a report to investigate the incident leading to the death of the resident. He referred the report to the hospital's quality assurance associate. As the report was created for quality assurance purposes, the health authority denied access under the *Evidence Act*.

Generally, s. 51 of the *Evidence Act* states that records arising out of quality assurance activities in hospitals or in mental health facilities are privileged and cannot be admitted into evidence in legal proceedings or disclosed to anyone other than those listed in the section. Section 51 makes it clear FIPPA does not override the *Evidence Act* privilege. In other words, if a record is protected by s. 51 of the *Evidence Act*, FIPPA does not apply.

During this review we examined the record and determined whether the health authority had appropriately applied s. 51 of the *Evidence Act*. The review included an examination of the contents of the record, the policies of the hospital outlining the quality assurance process and the specific process used in this case.

The health authority's policies and procedures demonstrated that it created a separate stream that is identified as quality assurance. This stream is apart from the other operations of the hospital, such as insurance and risk management. The separation of the quality assurance function made it easier to identify records appropriately covered by s. 51of the *Evidence Act*.

Further, the health authority demonstrated through its documentation that the record was created and considered only by the required authorities within the quality assurance stream, thus satisfying the requirements of s. 51 of the *Evidence Act*.

Records Related to a Decision to Restrict Use of a Power Wheelchair

A long-term care facility restricted a resident's use of a power wheelchair after a series of alleged mishaps and safety violations. The resident thought the restriction was unreasonable and requested relevant records from the medical chart, including any incident reports. The public body responded that it had no records relevant to the request and that the decision was "based on the course of events as outlined in [the resident's] medical chart." The resident did not believe that the chart was the source record for the

decision and asked us to review the decision to withhold the record.

The public body showed us specific areas of the medical chart that were relevant to the decision taken. However, it also managed to locate relevant incident reports, which it initially chose to withhold pursuant to s. 51 of the *Evidence Act*. Section 51 imposes a carefully structured series of requirements on hospitals that, if met, will provide absolute legal protection against having to disclose particular incident or quality of medical care reports. After some discussion, the public body agreed with us that s. 51 did not apply to the records in question and disclosed the chart and reports to the applicant.

Judicial Records in BC Archives

A researcher asked a public body for records pertaining to the "Patriation References", a set of four court cases seeking a judicial opinion on the constitutionality of a federal government proposal for unilateral patriation of the Canadian Constitution. In its response, the public body withheld a report by a former judge of the BC Court of Appeal on the basis that FIPPA did not apply to the report by virtue of s. 3(1)(a).

The applicant objected to the withholding of the report. Having reviewed the record and previous decisions of the Commissioner, we were inclined to agree with the public body's position.

The public body gave us a copy of a letter from the Court of Appeal in response to the public body's consultation regarding whether the record could be released. The letter outlined the purpose of the report and why the Court considered the report to be outside of the scope of the applicant's request. At our request, the public body consulted with the author of the letter and obtained consent for portions of the letter to be read to the applicant.

On that basis the applicant agreed that the judge's report fell outside of the scope of his request.

Records Relating to a Contract with a Health Authority

An applicant made a request to a health authority for records concerning the contract between the health authority and the applicant's former employer, a residential care facility.

The health authority decided to release a portion of the information, and advised the operator of the residential care facility accordingly.

The operator of the care facility objected to the health authority's decision to release records to the former employee of the facility. The applicant, who had filed a wage claim against the former employer, simply wanted to confirm the effective dates of the contract between the health authority and the facility. The Health Authority had intended to release this information.

The record in dispute was a one page "Contract Amendment Routing Slip" issued by the health authority regarding its contract with the company operating the residential care facility. The operator maintained that release would be harmful to his business interests and therefore must be withheld under s. 21 of FIPPA. He argued that the information that the health authority intended to release would reveal labour relations information and that disclosing the information to the applicant would bring about financial loss to the officers and directors of his company.

This office explained to the operator that his arguments against disclosure did not meet the standards for s. 21. The operator accepted our opinion that s. 21 did not properly apply to the record in dispute and the record was released.

Agreements between BC Rail and Canadian National Railways

Several parties requested copies of the records by which assets of BC Rail were transferred to Canadian National Railways. The requested records included the original Transaction Agreement, the Transaction Amendment Agreement resulting from the review by the federal Competition Bureau, and the Revitalization Agreement. Each document was lengthy and detailed and had many schedules.

The ministry proposed releasing the records with portions deleted to avoid harming the business interests of third parties, as required by s. 21 of FIPPA. One of the affected third parties objected to the release and asked us to review the ministry's proposed release.

The final agreements, as approved by the Competition Bureau, were subsequently made public with portions deleted under s. 21. The third party considered that the public release should be sufficient to satisfy the original applicants but the applicants wanted copies of the original agreements as they read before the amendments required by the Competition Bureau review.

The ministry agreed to conduct a line by line comparison of the original documents with the final approved documents to ensure that the same information was deleted from them as had been deleted for the public release of the approved documents. On this basis, the third party agreed to release of the original documents.

The applicants apparently were satisfied with this release as none of them asked us to review the decision of the ministry to delete information from the documents.

Complaint Letter about a Parent Sent to a School Board

A parent became aware that a letter of complaint concerning the parent had been sent to the principal of a local school. When this

information came to light, the parent discussed the issue with the principal and obtained a commitment that the letter would be sealed and not released to anyone. Subsequent to this, the parent requested a copy of the letter of complaint from the school district. The school district refused, stating that disclosure would be an unreasonable invasion of the privacy of the letter writer(s) and other people mentioned in the correspondence. The parent requested a review by the OIPC.

The school district told us that one of the factors considered in withholding the complaint letter was the apparent animosity between the various parents involved. The school district did not wish to escalate the perceived conflict.

After receiving the record at issue, it became apparent that the content of the record was seemingly innocuous. At our request, the school district approached the third parties to seek their consent to release the letter. All agreed and the letter was released to the applicant.

The Name of a Witness to a Death

An applicant made a request to a police department for records identifying the person who witnessed the death of his brother. In response, the police force withheld the name of the witness on the grounds that disclosure of this information would be a violation of the witness's personal privacy, as the information was collected as part of a law enforcement investigation.

The applicant was upset that information he perceived as vital had been withheld and asked us to review the matter.

FIPPA sets out the general principle that the disclosure of personal information compiled "as part of an investigation into a possible violation of law" is presumed to be an unreasonable invasion of a third party's personal privacy. While it is conceivable that circumstances could arise in which the general presumption could be overridden, the legal standard is set to protect the ability of the police to conduct investigations. In this case, the response from the police force was that names of third-party witnesses from the investigative files could not be disclosed under FIPPA. Given this reality, and after discussion of alternatives, the requester chose not to pursue the matter further with our office.

Declassification of Provincial Highways

The applicant asked a municipality for copies of all correspondence relating to its dealings with the provincial government about declassification of provincial highways within the municipality's boundaries – a sometimes-contentious practice also known as downloading, by which the province transfers to a municipality responsibility for road maintenance and upgrades. The municipality

withheld certain records on the grounds that release would harm its relations with the province, under s. 16 of FIPPA. The applicant requested a review by the OIPC.

Upon investigation, we took the position that the highways-related correspondence withheld by the municipality was uniformly professional in tone, character and content, and disclosure would not reveal confidential information from the province, nor otherwise be likely to cause any repercussion that would damage relations between the municipality and the province. The municipality ultimately agreed with this assessment and in the interests of transparency released the requested records.

Completion Date of Arena

A member of the media asked a city to provide an amended schedule for completion of an arena. The city told the applicant that it was not in possession of an amended construction schedule and suggested that the applicant contact the developer directly.

During mediation, the city at first advised us that any amended construction schedule, if it existed, was a record belonging to the developer and that it had no control over such records. However, after we reviewed with the city the relevant terms of the contract between the city and the developer regarding the city's ability to access the developer's records, the city agreed to resolve the matter by obtaining a copy of the amended construction schedule from the developer and providing it to the applicant as requested.

Investigating and Resolving Access Complaints

In addition to the right to request a review of a decision to sever or withhold information, people who have made access requests may file a complaint with the OIPC about the way the request was handled. If the dispute about an access request concerns a decision other than the decision to withhold or sever information, the matter is termed a "complaint."

Examples of complaint subjects include unreasonable access fees, delayed responses to access requests, inadequate searches for responsive records and inappropriate response time extensions. Although the 30-business day timeframe does not apply to complaints, a complaint should be filed at the earliest opportunity, since the OIPC may decline to investigate a complaint that has not been made in a timely fashion. Where a complainant has not already given the public body an opportunity to respond to and attempt to resolve the complaint, the OIPC will normally refer the complainant to the public body before the OIPC takes further action.

In 2004-2005, the OIPC received 219 complaints related to access requests, of which only three proceeded to a formal inquiry for resolution.

Table 4. Disposition of FIPPA Access to Information Complaints

Table 4 describes the access complaints resolved by the OIPC in the last fiscal year.

Type	Disposition									
	Mediated	Not Substantiated	Partially Substantiated	Substantiated	Referred to Public Body	No Reviewable Issue	Withdrawn	Notice of Inquiry Issued	Orders & Other Decisions	Total
Adequate Search[10]	8	16	2	4	14	0	0	1	1	**46**
Duty[11] Required by Act	28	36	3	5	32	10	6	1	3	**124**
Fees	11	6	1	2	9	0	3	1	0	**33**
Time Extension	9	2	0	1	2	0	2	0	0	**16**
Total	**55**	**60**	**6**	**12**	**57**	**10**	**11**	**3**	**4**	**219**

10 Whether all responsive records were accounted for in the public body's response.
11 S. 6 requires a public body to respond to an access request openly, accurately and without delay.

Table 5. Disposition of FIPPA Access and Privacy Complaints

Table 5 shows the types of both access and privacy complaints closed by public body for 2004-2005.

Public Body	Disposition									
	Adequate Search	Collection	Correction	Disclosure	Duty Required By Act	Fees	Retention	Time Extension By Public Body	Use	Total
Insurance Corporation of BC	1	2	1	5	13	2	0	3	0	**27**
Ministry of Human Resources	2	1	2	4	11	0	0	1	0	**21**
Workers' Compensation Board	0	1	1	7	3	0	1	0	1	**14**
Provincial Health Services Authority	4	0	0	0	8	1	0	1	0	**14**
Ministry of Health Services	3	0	0	2	5	1	0	0	2	**13**
Ministry of Public Safety and Solicitor General	2	0	0	0	6	4	0	1	0	**13**
Ministry of Children and Family Development	1	1	1	2	5	0	0	2	0	**12**
Vancouver Police Department	2	0	2	1	4	0	0	1	0	**10**
University of British Columbia	0	4	0	1	0	3	0	0	1	**9**
Ministry of Attorney General	3	0	0	3	1	0	0	0	1	**8**
All Other Public Bodies	28	15	1	26	68	22	2	7	5	**174**
Total	**46**	**24**	**8**	**51**	**124**	**33**	**3**	**16**	**10**	**315**

Case Summaries: FIPPA Access Complaints

Fees Relating to Records of a Visit by the Dalai Lama

During the spring of 2004 several prominent world spiritual leaders participated in a number of events in Vancouver, including several at local universities. A newspaper reporter requested the itemized list of expenses incurred by one of the universities for hosting the visits of His Holiness the Dalai Lama, Archbishop Emeritus Desmond Tutu, and Professor Shirin Ebadi.

The university responded with a fee estimate for $1,597.50, representing 56 hours of work to locate, copy and prepare the records for disclosure. It estimated the response would be approximately 30 pages.

At the time of the request, the university had not finished collecting and compiling the financial information from the various organizations involved. It took the university several months to gather all the necessary information.

After mediation with this office, the university agreed to release, at no cost, the detailed list of expenses and revenues and the reporter was able to write his story.

Witness Statements Missing from Police Files

An applicant requested the applicant's police file from a police department. When it was provided, the applicant noted that no witness statement had been provided, although other records mentioned that the investigating officer had asked for one. Also it was noted that information that the applicant had previously requested be annotated to the file was not disclosed.

The applicant complained to us that the police had not fully responded to the request and had not appropriately annotated the file as required by s. 29 of FIPPA. That section gives citizens the right to request a correction of their personal information. If a public body chooses not to make the correction, FIPPA requires them to annotate the file with the correction that was requested but not made.

At our request, the police reviewed the possible locations for the witness statement and concluded that, although asked for, a statement was never taken. The police could not determine why the annotations were not on file. They confirmed by letter to both the OIPC and the applicant that, if the applicant provided additional copies, they would ensure that the annotations would be placed on file for future requests. The applicant was satisfied with the outcome.

Missing Consultant's Report

A complainant requested an engineering report done by a consulting firm for a municipality. The municipality conducted a search but was unable to locate the document. The complainant asked us to investigate, as he believed the municipality must have had a copy.

During mediation, the municipality provided details of the search it conducted for the report. The OIPC determined that the search was extensive enough to meet the requirements of the Act.

However, after further discussion, the municipality agreed to contact the consulting firm and find out the cost of obtaining another copy of the report. The municipality received a copy of the report and provided the applicant with his own copy.

Delay in a Response by an Improvement District

A complainant asked the board of the improvement district where he resided for financial information about a project that the district was contemplating. Although the Act requires a public body to respond within 30 days, the board did not respond for an extended period of time. The complainant asked the OIPC to contact the district on his behalf.

During the investigation, it became clear that the members of the board were not aware of their legislative obligations, for a variety of reasons. After the request was made, the volunteer board members had changed and no one had followed up on the request. The new secretary lived out of the province and only resided in the district for holidays. The complainant understood the volunteer nature of the board members' work and was willing to wait for the records. With the assistance of the OIPC, the district was able to provide some of the requested records but others contained legal advice and were appropriately withheld. The complainant was satisfied with the outcome.

Records Relating to the Sale of Tobacco to Minors

An applicant requested records from a health authority relating to investigations of certain convenience stores for compliance with the laws prohibiting sales of tobacco products to minors. The health authority provided only a small number of records to the applicant.

The applicant, believing more records should exist, filed a complaint with the OIPC. As a result of mediation it was discovered that part of the problem was that the enforcement branch responsible for conducting the compliance investigations did not understand that its records were subject to the provisions of FIPPA. The health authority rectified this misunderstanding and a large number of records responsive to the original request were subsequently released to the applicant.

Orders and Other Decisions

If a review or a complaint matter cannot be resolved through mediation it may proceed to a formal inquiry. The mediation process is completely separate from the inquiry process. The Commissioner has not been involved in nor is he privy to any of the discussions that occurred during the mediation phase. This is to ensure that, if the matter proceeds to an inquiry, the Commissioner is not perceived to be biased and can approach the matter with an open mind.

The Commissioner has the power to hold inquiries and decide all matters of question and fact and to dispose of the matter by issuing an order under s. 58 of FIPPA. Inquiries can either be written or conducted in person. Most inquiries are written inquiries.

At an inquiry, both parties provide initial submissions outlining their perspective and argument on the matter under review. Those submissions are exchanged between the parties, and each party is given the right to reply. If the material in the submissions is confidential or sensitive, all or parts of that submission may be submitted *in camera*, which means that only the Commissioner will see that information.

At the end of an inquiry, the Commissioner will issue an order and the order becomes a public document. All orders are published on the OIPC website at www.oipc.bc.ca. If the order is a matter concerning personal privacy, the orders are anonymized.

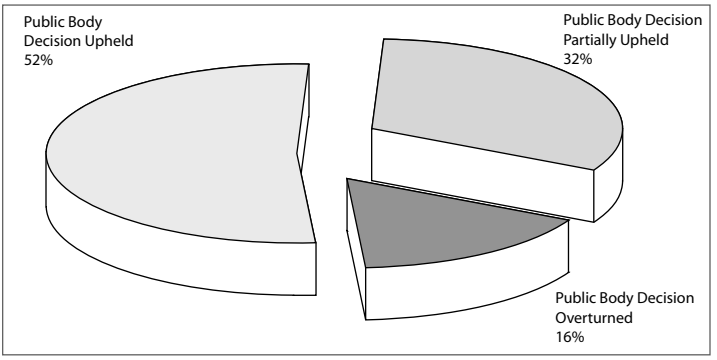
In making an order, the Commissioner has a number of options, including:

- Requiring the public body to release more information
- Confirming the decision of the public body to withhold information
- Requiring the public body to refuse access to information
- Confirming, excusing or reducing a fee
- Require that a duty imposed by the Act be performed
- Require a public body to stop collecting, using or disclosing information or to destroy information.

In 2004-2005, forty-four matters were concluded by way of a formal inquiry.

The OIPC has now hired a full-time Adjudicator.

The following chart illustrates how matters were resolved by order in 2004-2005:



Summaries of Select Orders

The following is a small sample of the binding access to information appeal decisions, or "orders", the OIPC issued in 2004-2005.

Order F05-05—Contractor Records in the Custody of the Forensic Psychiatric Services Commission

The Forensic Psychiatric Services Commission is established under the *Forensic Psychiatry Act* to provide inpatient and outpatient forensic services for mentally ill persons who have come in contact with the criminal justice system. As part of an accreditation process, a consulting firm was hired to perform a number of special services on behalf of the Commission. In turn, the consulting company hired an individual to perform the services.

The applicant made an access request for records relating directly or indirectly to the retainer of the contracted services. In response to the request, the Commission provided some records but withheld information relating to time estimates, daily rate information, total fees, administrative expenses and standard contract terms and conditions.

The consulting firm argued that the financial and commercial information was provided in confidence and that disclosure would allow competitors to undercut it on the pricing component of future tenders or proposals. It argued the information should be withheld by virtue of s. 21 of FIPPA which requires a public body to withhold information if disclosure of that information would significantly interfere with the competitive position of a third party.

The adjudicator found that the information did not meet the three-part test contained in s. 21 of FIPPA and ordered release of all of the information withheld under s. 21.

Order F05-02—Investigative Records Concerning Bullying at a School

During a particular school year, the applicant's daughters complained to their mother about a series of incidents that they said happened at school, involving a teacher and several other students. The mother complained to the school on her daughters' behalf. The School District arranged for two investigations, one into specific allegations involving the teacher, and one regarding more general concerns about harassment and bullying at the school. Following the investigations, the applicant asked, under FIPPA, for full copies of the reports that resulted from the investigations.

In preparing its response, the school district gave notice to the teacher that it intended to release portions of the report, in severed form. The teacher objected that the school district's proposed release package was inadequate to protect his/her privacy and thus in contravention of s. 22.

The adjudicator found the School District was authorized to withhold some but not all of the information in the reports. In ordering further release, the adjudicator determined that information related to normal or typical workplace activities was not protected information, nor was any third party personal information contained in the reports supplied by or about the mother or the daughters in the course of the investigation.

F04-17—A Request for the Premier's Phone Records

The applicant made a request for access to "records for all of the Premier's personal and official phone lines" for a specified period. These included "all fax, telephone, and cellular telephone logs, both long distance and local, and the long distance telephone bills for that time."

In response the Ministry of Management Services severed information on the grounds that disclosure could reasonably be expected to create security risks (s. 15) and harm the economic interests of the Government of British Columbia (s. 17).

During mediation, the applicant abandoned his request for the Premier's private telephone calls in Victoria or Vancouver, and the ministry abandoned its position that disclosure would create a security risk.

At inquiry, the applicant argued the information should be released in the public interest. He argued that very few calls were "truly personal", but "government-to-government and business phone contacts are the public's affair…"

The Commissioner found that s. 17 did not apply to any of the information in dispute. However, the Commissioner did find that disclosure of the phone logs would constitute an unreasonable invasion of privacy of third parties.

F04-06—Ministry Refuses to Disclose Information from Computer Consulting Services Contracts

The Ministry of Health received an access request from an unsuccessful proponent for a variety of records related to the contract proposals submitted by three successful proponents. In response, the ministry identified 100 pages of responsive records, from which it withheld all or portions of 71 pages on the grounds that disclosure would harm the financial interests of the ministry and the successful proponents. The ministry also withheld the names of the employees named in each proposal as it believed FIPPA required this information to be withheld.

The applicant believed there was a lack of transparency in the process. He stated that, despite his requests, the ministry did not explain what was lacking in his proposal.

The information in dispute included the daily fee rate, the maximum fees payable, the proposals themselves and the score sheet used to evaluate the proposals.

The Commissioner did not believe a clear connection existed between disclosure of the information and a resultant harm to either the ministry's or the third parties' financial interests. With the exception of the personal information, the Commissioner ordered the ministry to disclose all of the disputed information to the applicant.

The Basic Rules of Public Sector Privacy

As mentioned earlier, under the F*reedom of Information and Protection of Privacy Act (*FIPPA*)*, public bodies must adhere to a set of rules governing the collection, use and disclosure of personal information. These are known as "fair information practices". These rules guide public bodies in determining what personal information may be collected, how it should be collected, what it can be used for and to whom it can be disclosed.

Public bodies are not permitted to indiscriminately demand personal information from citizens. Personal information may be collected only if authorized by law, for law enforcement purposes or if the information relates directly to and is necessary for an operating program or activity of the public body. The principle underlying this rule is that of necessity and relevance in the collection of personal information. The idea is to limit the collection of information to only that which is necessary to perform the function or service.

With limited exceptions, public bodies must collect personal information directly from the individual the information is about and tell that individual why it is being collected, how it will be used and the authority under which it is collected. This ensures that public bodies are transparent about their data practices and discourages the creation of secret government databases.

Under FIPPA, public bodies must take all reasonable steps to ensure the information they collect is accurate and complete. This is because decisions based on inaccurate or out-out-date information may have potentially devastating consequences to an individual, such as denial of service, revocation of a licence or permit or unwarranted investigations. The requirement that personal information be accurate and relevant is even more important in the context of networked databases, where information, both accurate and inaccurate, can be widely and irretrievably transmitted in seconds.

Public bodies must retain an individual's personal information for a minimum of one year after it is last used to make a decision that directly affects the individual. This gives individuals some opportunity to get access to their own information to see if it is accurate and complete.

Public bodies are required to use personal information only for the purpose for which it was collected. This rule is one of the most important privacy protection rules. It imposes reasonable limitations on the use and disclosure of personal information, such limitations being the bedrock of information privacy protection. It means public bodies can generally only use and disclose information for the purpose specified at the time it was collected—the primary, or original, purpose.

FIPPA does permit other uses of personal information, but only if they are consistent with the original purpose for collection. To be consistent, the secondary use must have a reasonable and direct connection to the original purpose for collection and must be necessary for performing the statutory duties of the public body or operating a legally authorized program of the public body. For example, health information collected by a hospital to assist in treatment decisions would be a primary use. The hospital could not use that information to identify cancer patients and target them for donations to a cancer clinic. That would be an inappropriate secondary use of the information, which could only be undertaken if affected patients consented to that new use.

FIPPA sets out the only circumstances in which a public body may disclose personal information, including if the individual has consented, for the purposes of law enforcement, for the purpose for which it was obtained, to collect a debt, or if the information is necessary for the delivery of a common or integrated program.

Finally, public bodies are required by law to take all reasonable steps to ensure the personal information they have collected is protected from unauthorized collection, use and disclosure. This includes, for example, physical file security, staff training, encryption software and password protection. With identity theft growing by leaps and bounds, this duty is more and more important.

Investigating and Resolving Privacy Complaints

Individuals who believe their personal information has been inappropriately collected, used or disclosed contrary to FIPPA may ask the Commissioner to investigate. As with access complaints, where a person has not demonstrated they have attempted to resolve their privacy complaint with the public body, the OIPC will generally refer the complainant back to the public body so that they can attempt to resolve the complaint. If the complainant has done this and remains dissatisfied, the complainant may file a complaint with the OIPC, which will examine the matter and determine whether further investigation is warranted.

Privacy complaints are assigned to OIPC Portfolio Officers. They have delegated authority to investigate and resolve those complaints either through mediation or by finding the complaint substantiated, unsubstantiated or partially substantiated. In this process, the Portfolio Officer examines all of the circumstances concerning the complaint, the legislation and relevant orders and discusses the matter with the complainant and the public body. If the complaint is determined to be wholly or partially substantiated, the Portfolio Officer will work with the public body to ensure that the problem

is corrected or that steps have been taken to reduce the risk of a recurrence. Solutions may include changes in policies, procedures, training, technological fixes or a combination of any of these.

The OIPC closed 96 privacy complaints concerning the public sector in 2004-2005.

Table 6. Disposition of FIPPA Privacy Complaints

Complaint Type	Mediated	Not Substantiated	Partially Substantiated	Substantiated	Referred to Public Body	No Reviewable Issue	Withdrawn	Declined to Investigate	Total
Collection	3	2	0	1	15	3	0	0	**24**
Correction	0	1	0	0	7	0	0	0	**8**
Disclosure	6	11	2	4	20	3	4	1	**51**
Retention	0	1	0	1	1	0	0	0	**3**
Use	1	2	0	1	5	1	0	0	**10**
Total	**10**	**17**	**2**	**7**	**48**	**7**	**4**	**1**	**96**

Table 6 shows the number of complaints closed by the OIPC and the manner in which those complaints were resolved.

Case Summaries: FIPPA Privacy Complaints

Disclosure of Personal Information to an Employer by the WCB

During the course of an appeal process, a public body released personal information of a claimant to the claimant's employer. The employer had initially disputed the claim but then chose not to take part in the process. The public body wrote to the claimant stating that only the adjudicator's report had been released. Nonetheless, the claimant filed a complaint that the public body had inappropriately released her personal information to her employer.

The OIPC investigated the matter by obtaining copies of all records in the claimant's file, reviewing the public body investigation report provided to the applicant and examining the public body's policies related to this issue. The investigation revealed that only the final decision reports were released in the interests of administrative fairness to the employer, as a party to the appeal, for the purpose of ensuring that the employer could take part in the process at any stage if he or she wished. Further the public body's governing act restricts an employer's use of claim information only for the purposes of adjudicating a claim.

The OIPC found that the complaint was unsubstantiated.

Complaint about Public Disclosure by a Police Department

Counsel for an individual complained that a police department had issued a public warning about his client. A special sexual offence unit issued the warning. While the individual in question had a criminal past, that past did not include any sexual offences. Counsel for the complainant said that the public warning was misleading and had caused his client considerable grief.

The Portfolio Officer examined the complaint and found, that, while the text of the warning was accurate, the fact that it was issued by the sexual offence unit was, in these circumstances, misleading. In order to be fair to both the offender and to the public, any public warning should be clear and accurate. The police department agreed to take steps to ensure any future notices were issued by the police generally, and not by any specific unit.

Collection by a Health Authority of Information about Firearms in Home-Care Risk Assessments

After being released from the hospital following knee surgery, a complainant received home-based physiotherapy services from the Community Care Program of a health authority.

Workers' Compensation Board regulations required that, before providing home-based care, the physiotherapist first conduct a risk assessment of the patient's home. As part of this process, the physiotherapist asked the patient a series of standard questions. One of the questions concerned the presence of weapons or firearms in the house. The patient wrote a letter of complaint to the health authority, stating the collection of this information violated his privacy. He requested that the questions about firearms be removed from the risk assessment form and all information collected about the possession of firearms in the files of all community care clients be destroyed. The health authority explained it was necessary to retain this information for risk assessment purposes, but also stated it would be conducting a review of the risk assessment form. The complainant was not satisfied with the explanation and asked us to investigate.

While our investigation was in process, the health authority completed its own review, determined that collecting information about firearms was not necessary and decided to stop collecting this information. We found the complaint was substantiated. The health authority also agreed to revise its standard forms to remove any reference to firearms.

With respect to the complainant's request to destroy any references to firearms previously collected, the health authority declined. They maintained that any information already housed in client files must legally remain intact to maintain the integrity of the health record. It did, however, adopt security procedures to allow only community caregivers access to the information in the record.

A Special Privacy Analysis—Privacy Implications of the USA Patriot Act

If a privacy complaint concerns matters of a systemic nature, one that affects a large number of people or one that is of substantial public interest, the findings of the investigation may result in a public investigation report. This year, the OIPC conducted one large-scale public investigation into the privacy implications of the *USA Patriot Act*.

Early last year, the BC government decided to outsource the administration of the BC Medical Services Plan to Maximus, through a company located in British Columbia but owned by a US-based corporation. Soon after, a lawsuit was filed alleging, among other things, that the outsourcing to a US-linked service provider unlawfully exposed the health information of BC residents to access under the *USA Patriot Act*.

The *USA Patriot Act* was enacted after the events of September 11. That Act eased some of the restrictions on foreign intelligence gathering within the United States and provided the US intelligence community with greater access to information. Section 215 allows the FBI to obtain a court order under the *Foreign Intelligence Surveillance Act* (FISA) to obtain "any tangible thing," which includes information. Prior to the enactment of the *USA Patriot Act*, FISA orders could be obtained only where the FBI showed specific facts giving reason to believe that the person the records are sought about was a foreign power or an agent of foreign power. Section 215 lowered that threshold to allow the FBI access to information if it was necessary for an authorized investigation to obtain foreign intelligence information to protect against international terrorism.

An order under section 215, or a national security subpoena, is issued and executed in secret. The *USA Patriot Act* prohibits anyone who has been required to produce information from disclosing to any other person (other than those persons necessary to produce the information) that the FBI has sought or obtained the information.

There are a number of rules public bodies must follow to protect the privacy of BC citizens. Section 30 of the *Freedom of Information and Protection of Privacy Act* (FIPPA) requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. Section 33 of FIPPA prohibits the disclosure of personal information, except under the expressly listed conditions.

In May of 2004, the Commissioner announced that he would conduct a public consultative process and then consider two questions relating to the *USA Patriot Act* and outsourcing of public services. The two questions were:

1. Does the *USA Patriot Act* permit US authorities to access the personal information of British Columbians that is, through the outsourcing of public services, contracted to US-linked companies?
2. If it does, what are the implications for public body compliance with the personal privacy protections in FIPPA? What measures can be taken to mitigate these risks?

After careful study and extensive analysis, the OIPC's October 2004 report concluded that, under section 215 of the *USA Patriot Act,* the FBI could issue an order to a person subject to the court's jurisdiction compelling that person to obtain records or other things located outside the US, but under the control of that person, and deliver them to US authorities in the US. This would involve the US court's order reaching beyond the US and ordering, without the intervention of Canadian law or constitutional principles, much less Canadian courts or other authorities, the disclosure of information located in British Columbia.

We also concluded that disclosure by a contractor or a public body for the purpose of complying with such an order would be an unauthorized disclosure of personal information under ss. 30 and 33 of FIPPA.

The OIPC's report also considered what reasonable and effective mitigating measures could be taken to address *USA Patriot Act* risks.

The report did not recommend a ban on outsourcing of government services to private sector contractors, an outright ban on outsourcing being neither necessary nor practicable. Nor did the report recommend that corporations with links to the US sufficient to place them at risk of a *USA Patriot Act* order be discriminated against in competing for outsourcing work.

The OIPC's report recommended, instead, that FIPPA be amended to prohibit disclosure of personal information located in British Columbia in response to a foreign court order, warrant or subpoena, a prohibition that would apply whether the order is issued by a US court or court of any other country. This recommendation was made because there are clear indications in US cases that an American court may well give effect to such a legislative prohibition in British Columbia law and, as a result, not order production of personal information from abroad in the first place.

Another recommendation was that contractual arrangements be implemented in any outsourcing of public services that involves personal information to ensure that persons subject to US court jurisdiction do not have legal or practical control over personal information located in British Columbia. Such measures are desirable because a US court will issue a disclosure order only if it is satisfied that the person under its jurisdiction has control over foreign-located records in the first place. The provincial government promised to follow this recommendation at

the provincial level and has since said that its outsourcing initiatives to date, which include the outsourcing of our health plan, have included such protective measures.

The investigation report recommended that all public bodies in British Columbia ensure that they commit, for the duration of all relevant contracts, the financial and other resources necessary to actively and diligently monitor contract performance, punish any breaches and detect and defend against actual or potential disclosure of personal information to a foreign court or other foreign authority.

Another recommendation was that public bodies should not rely on contractors to self-report their breaches. Any public body that has entered into an outsourcing contract should create and implement a program of regular, thorough, compliance audits. A third-party auditor, selected by the public body, which has the necessary expertise to perform the audit and to recommend any necessary changes and mitigation measures, should perform such audits.

Another significant recommendation—as a decidedly interim measure—was that, pending nation to nation agreements to allow national security information to flow, the provincial government ensure that personal information in the control of public bodies in British Columbia is not located or accessible from outside Canada. This was necessary in order to ensure that the prohibition against disclosure of personal information in response to a court order issued by a foreign court was not rendered meaningless by the offshoring of personal data. This recommendation made its way into the legislation that was enacted before our report was released.

An Overview of the Personal Information Protection Act

Private sector privacy obtained legal protection in British Columbia on January 1, 2004, when the *Personal Information Protection Act* (PIPA) came into force. PIPA applies to more than 300,000 organizations in British Columbia, including businesses, unincorporated associations, trade unions, trusts and not-for-profit associations. Section 2 of PIPA states its purposes:

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

PIPA applies to personal information, which it defines as information about an identifiable individual. PIPA does not apply to business contact information or work product information.

PIPA does not apply to the collection, use or disclosure of personal information for personal, home or family purposes (for example, for Christmas card mailing lists of family and friends), for artistic or literary purposes or for journalistic purposes (this protects freedom of expression for the news media).

The Basic Rules of Private Sector Privacy

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

Consent for collection of personal information

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

Limits on collection of personal information

Organizations must collect personal information only for reasonable purposes and must collect only as much as is reasonable for those purposes. Unless PIPA allows it, organizations must collect personal information directly from the individual concerned and tell the individual how they intend to use and disclose the information at or before the time the information is collected.

Use and disclosure of personal information

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

Access to personal information

On request, an organization must provide an individual with information about the existence, use and disclosure of the individual's personal information and provide access to that information unless PIPA excuses the organization from giving access in whole or in part. Also on request, and where satisfied on reasonable grounds, an organization must correct information that is inaccurate or incomplete. Organizations may charge a minimal fee for responding to a request for access, but the fee should not be a barrier to access.

Accurate and complete personal information

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

Designate a Privacy Officer

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

Policies & Procedures

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

Resolution of Complaints

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

Special Rules for Employment Relationships

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

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

Personal information does not include "business contact information", which is an individual's name and position or title, business telephone number, business address, business e-mail, business fax number and other business contact information. It also does not include "work product information", which is information prepared by individuals or employees in the context of their work or business. Work product information does not include personal information about other individuals. For example, an employee performance report prepared by a management employee of a company would be work product information as it relates to that management employee, but the personal information about the employee being assessed would be the personal information of the other employee.

Organizations are not required to seek consent from employees for the collection, use and disclosure of employee personal information, provided the information is collected for the purpose of establishing, managing or terminating the employment relationship.

The Appeal and Complaint Mechanism

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

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

A dispute concerning access to information or the correction of personal information is termed a "review" and must be requested within 30 business days after the organization's decision.

A dispute concerning the collection, use and disclosure of personal information, fees or disputes or any other thing is termed a "complaint". PIPA does not impose a time limit for making a complaint, but, unless there are extenuating reasons, the OIPC will not generally allow a complaint made more than six months after the individual concerned had notice of the circumstances.

The OIPC will generally defer or adjourn acting on a complaint or request for review until the individual concerned shows that he or she has communicated directly with the organization and enabled it to respond to or attempt to resolve the matter.

In 2004-2005, the OIPC received 53 reviews and 156 complaints under PIPA and closed 52 reviews and 118 complaints.

Table 7. Disposition of PIPA Complaints

Table 7 illustrates the types of PIPA complaints resolved and closed between April 1, 2004 and March 31, 2005.

	Disposition								
Type	Mediated	Not Substantiated	Partially Substantiated	Substantiated	Referred back to Organization	No Reviewable Issue	Withdrawn	Notice of Inquiry Issued	Total Files Closed
Adequate search	2	2	1	0	1	1	0	0	**7**
Collection	4	3	0	0	16	4	3	2	**32**
Correction	1	1	0	0	0	0	0	0	**2**
Disclosure	4	1	21	1	1	4	0	0	**32**
Duty Required by Act	11	4	2	1	10	5	0	0	**33**
Fees	1	0	0	0	1	0	0	0	**2**
Use	1	1	0	0	7	1	0	0	**10**
Total	**24**	**12**	**24**	**2**	**36**	**15**	**3**	**2**	**118**

Of the 53 requests for review received under PIPA, the OIPC closed 50. Most of those reviews concerned requests for personal information that had not been responded to within the 30-day legislative timeframe, also known as "deemed refusals."

Table 8. Disposition of PIPA Requests for Review

Table 8 illustrates how the 52 review files were closed in fiscal 2004-2005.

	Disposition						
Type	Mediated	Referred back to Organization	No Reviewable Issue	Non Jurisdictional	Withdrawn	Notice of Inquiry Issued	Total Files Closed
Deemed Refusal	27	4	1	0	2	0	**34**
Deny Access	3	2	2	1	0	0	**8**
Partial Access	4	1	1	0	1	3	**10**
Total	**34**	**7**	**4**	**1**	**3**	**3**	**52**

Case Summaries: PIPA Privacy Complaints

The OIPC has a long history of successfully mediating privacy disputes in the public sector and is applying that experience to PIPA disputes. Summaries of recent PIPA mediations follow.

Personal Information Properly Withheld by Society

A non-profit society received a request for personal information from a former board member. The responsive records also included records of complaints both by and about the applicant board member. Some personal information of the applicant was released but other records were withheld or severed to protect third-party personal information, including the identity of certain third parties. The OIPC explained to the applicant that, as the identity and personal information of another individual must not be disclosed under PIPA, the organization had acted appropriately. The applicant was satisfied with the outcome.

Restaurant Releases Personal Information to Former Employee

A former employee of a restaurant asked for his employee information. Not being familiar with PIPA, the restaurant ignored the request. After being contacted by our office, the organization was prepared to release all of the applicant's personal information but was not sure how to proceed. We provided training and assistance, and the records were released. The applicant was satisfied with the outcome.

Private Recreational Facility Releases More Information

A member of a recreational facility was involved in an altercation with another facility user over the use of equipment and requested access to all of his personal information held by the facility. The records included email and other correspondence of the applicant, staff of the facility and other members. It also included incident reports relating to the altercation. The applicant received copies of the records, but some information was withheld under s.23(4)(c) of PIPA on the ground that it was the personal information of other individuals. Some of the information withheld included information about the applicant that was interwoven with other individuals' information.

As a result of OIPC mediation, the facility agreed to release more information. In some cases, this comprised the identities of staff and other information in records created by the staff of the facilities. In other cases, it was possible to separate the personal information of the applicant from the personal information of other individuals. The applicant accepted that the remaining information withheld was properly withheld.

Retailer's Notice Not An Attempt to Deliberately Mislead Customers

A clerk at a retail outlet asked for the complainant's telephone number when she was making a purchase. The clerk explained the benefits of providing her telephone number (including being entered into a draw for prizes) and assured her that her personal information would not be sold. There was a notice of collection posted at the checkout desk explaining the purposes for which the telephone number was being collected. The complainant read the first part of the notice and provided her telephone number. On a later visit to the store, she read the notice carefully and decided not to give out her telephone number and to communicate her wish to have the store delete her telephone number from its records. The focus of her complaint was that the wording of the notice was misleading and that, in accordance with s. 7(3)(b) of PIPA, her consent had not been validly given.

The first part of the notice indicated that the purpose of collecting the telephone number of customers was for marketing. In the second part, the retailer promised not to call customers. In the third part, the notice indicated that the retailer might send marketing material to customers through the mail. The retailer said that its choice of words, the structuring of the ideas and use of typefaces in the notice attempted to communicate this information in a way that would be most useful for customers.

Regarding the question of whether the notice was misleading, there was no evidence that the retailer was deliberately trying to mislead its customers about how their telephone number would be used. In applying the reasonable person test with respect to whether the retailer provided "false or misleading information", we concluded that a reasonable person would not believe the retailer deliberately provided false information or deliberately attempted to mislead its customers. The retailer agreed, however, to modify its sign to make the notification more clear.

The complainant accepted the outcome of our investigation.

Corner Store Reasonably Sought More Identification From Credit Card Customer

A complainant had tried to purchase a few items from a corner store using a major credit card. The checkout clerk asked the complainant to provide more identification so she could confirm that the complainant was the owner of the card, as the store had considerable experience of credit card fraud. The complainant refused to provide the additional identification and complained to that the corner store was attempting to collect personal information contrary to PIPA.

Section 11 says an organization can only collect personal information for purposes that a reasonable person would consider appropriate in the circumstances. Section 7(2) says an organization cannot, as a condition

of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service.

As for the appropriateness of the collection, a reasonable person would consider it appropriate for a retailer to confirm that a customer is the authorized credit card holder before processing a credit card purchase. In light of the possibility of credit card fraud generally, it was reasonable for the retailer to ask for more identification to ensure that the customer was the authorized credit card holder. We concluded there was no violation of s. 11.

As for the retailer requiring further identification as a condition of selling the goods, because verification of the identity of the cardholder was reasonable, its collection and use of identifying personal information did not go beyond what was necessary to provide the products the complainant wished to purchase.

The complainant was satisfied with the outcome.

Lease Agreement Did Not Provide Consent to Disclosure of Time-Share Owners' Personal Information

The applicant held a time-share in a resort development that had close to 20,000 time-share owners. He disagreed with the operating organization's decision to change the conditions of the time-share to prohibit smoking in any of the time-share units. He wanted to form an association of time-share owners and asked the organization to disclose the names and contact information of the lessees. The organization denied access to the information, citing PIPA.

The OIPC told the applicant and the organization that PIPA does not permit the organization to release the requested personal information. The applicant had argued that Article 18 of the time-share lease agreement provided implied consent by each lessee for the operator to disclose their names and contact information for the purpose of forming an association. Article 18 required the organization to assist in the formation of any lessee association. The OIPC felt Article 18 did not provide implied consent by lessees to disclosure of their personal information, particularly since the purpose of Article 18 could be achieved without the release of the personal information the applicant requested.

The organization indicated that it might be prepared to assist in the formation of a lessees' association by sending notices to each lessee. The organization is required to provide a budget to every lessee each year and it said that it could include the notice with the budget mail-out. The applicant would have to bear the costs of printing the notices. The organization said the notice would have to be in a form acceptable to the organization and relate only to the formation of a lessees' association. The applicant was satisfied with this outcome.

Hotel Acknowledges Improper Disclosure of Guest's Personal Information

A man complained that an employee of a hotel had inappropriately disclosed his personal information by informing his former wife of his stay at the hotel with a companion.

The hotel manager was aware of PIPA and that the hotel has a privacy policy in place. The manager acknowledged that the disclosure of this personal information breached PIPA. He circulated a memo to the hotel staff reminding them of PIPA's requirements and their obligation to keep guest information confidential. He also offered, on behalf of the hotel, to reimburse the complainant the cost of his stay, including the cost of his room and the meal he purchased at the hotel. The hotel then sent a letter of apology and reimbursed the complainant.

Physiotherapy Clinic's Fee for Copy of Patient's Records Accepted

A woman complained that a physiotherapy clinic breached s. 32(2) of PIPA by attempting to charge her more than a "minimal fee" to provide copies of her personal information held by the clinic. The clinic had quoted a fee of $25 for the first five pages of records and $1 for each additional page.

The complainant accepted our view that the revised $15 flat fee that the clinic proposed was within a range that could reasonably be considered "minimal" considering the time the clinic expended in locating the records and in attempting to determine the fee.

Public Consultations on Employment Privacy Issues

Privacy issues arising from the employment relationship are becoming both increasingly complex and pressing. Employees spend a large percentage of their waking hours at work and it is well recognized that they have an interest in privacy in the workplace. At the same time, employers have a business interest in monitoring employee activity in order to address a variety of concerns, ranging from detecting and deterring employee theft to ensuring a safe and harassment-free workplace. Technological advances will continue to provide employers with a wide range of monitoring options, many of which can operate without the employees' knowledge.

In the past, employee privacy concerns have been addressed in the decisions of labour arbitrators, in human rights decisions and, to a lesser extent, through the common law. In an effort to define the content of an employee's right or claim to privacy, decision makers have looked to a variety of sources, including the *Canadian Charter of Rights and Freedoms*, provincial legislation regarding privacy and human rights, and specific employment agreements. While each case turns on its specific

facts and the particular legislative framework involved, a number of principles have been consistently recognized throughout Canada. In addition, various bodies around the world that are charged with examining privacy issues have attempted to outline principles which should be recognized in addressing employment privacy concerns.

Last year the OIPC produced a draft resource document on selected employment privacy guidelines. We sought comment from a wide range of stakeholders, including business associations, labour organizations and privacy and civil liberties groups. The purpose of the resource document was to address certain privacy issues in the employment context in light of PIPA's special rules on employee personal information. The document was intended to be a pro-active resource for employers and employees, to assist them in dealing with three representative workplace privacy issues—the collection of information in the pre-employment context; the electronic monitoring of employees (including video, telephone and voicemail surveillance, as well as computer and email monitoring); and the collection of personal information through drug and alcohol testing.

We received extensive feedback. With the exception of pre-employment collection and use of personal information, there was little consensus in the feedback on our consultation draft. Having considered how best to assist in this area, the OIPC is in the process of finalizing a document of FAQs for pre-employment hiring practices, which will soon be circulated for comment again. Our goal is to build consensus and give practical advice, recognizing that the small and medium enterprises so important to our economy may particularly benefit from this guidance. If the FAQs prove popular, the OIPC will consider addressing other employment privacy issues in similar future documents.

Working Together

Most of the work of the OIPC is necessarily reactive. The bulk of the work that is done within the OIPC involves resolving complaints and appeals filed by citizens under both the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA).

However, a smaller but perhaps more critical role the OIPC plays is to comment proactively on any matter affecting access and privacy rights within and outside the province. The Commissioner has a role in relation to government and, to a certain extent, the private sector with respect to ensuring that new initiatives are appropriately restrained in the collection and use of personal information and to ensuring that the public's right of access is not diminished by new ways of doing business.

Under s. 42 of FIPPA, the Commissioner has the authority to comment on how proposed policies, programs, legislation, data-matching schemes, automated information management systems and outsourcing arrangements impact on the access and privacy right of BC citizens.

The Commissioner has similar responsibilities under PIPA. Last year we updated our website to add information concerning the prevention of identity theft in order to assist businesses in protecting the personal information they have collected.

In this general role, we commented on a number of initiatives, including:

- Federal government proposals for Internet and email interception laws by law enforcement authorities
- Digital rights management proposals
- Archiving of the records of the Open Learning Institute
- Grade 8 and 9 Health and Career Education Curriculum
- Privacy implications of the *USA Patriot Act*
- Who can act on behalf of a child with respect to access requests
- Privacy policy for online voter registration
- Providing lists of parents to Parent Advisory Committees
- Sharing member lists with members of a private club
- Publication of public officials' salaries
- Consent forms in the insurance industry
- Scope and intent of the public interest override under s. 25 of FIPPA
- Population-based registry of children with hearing loss
- Mechanisms for retrieving information that had been inadvertently disclosed
- Access to school counselling notes.

Educating the Public

Another small but very important role of the OIPC is to inform the public as well as public bodies and organizations about their access and privacy rights and obligations under FIPPA and PIPA. These activities include keeping the OIPC's website current and easy to access; meeting with interest groups and stakeholders; participating as keynote speakers and panellists at conferences, seminars and other public forums; lecturing at colleges and universities; delivering training seminars; distributing informational materials and engaging in dialogue with the media.

Last year, the main thrust of our educational activities involved PIPA and educating organizations and the public about private sector privacy. As one example, the OIPC website was extensively updated last year to reflect our new responsibilities under PIPA. Included on the new website are compliance tools for businesses and other organizations, guides to the legislation, tips on creating privacy policies and links to other private sector privacy resources and guidelines and complaint forms for consumers and employees.

The following is a small sample of educational activities conducted by the Commissioner and OIPC staff in 2004-2005:

Freedom of Information and Protection of Privacy Act Presentations

- Freedom of Information Training with the Saanich and Abbotsford Police Departments, Victoria
- Video surveillance presentation at the Provincial Facilities Workshop, Vancouver
- Health privacy presentation, Health Privacy Conference, Calgary
- Open Government and Protection of Privacy Speech, Simon Fraser University Department of Political Science, Burnaby
- Basics of Making an Access Request, presentation to Editorial Board of the Surrey Leader, Richmond
- Speech on Access to Information, BC Legislative Internship Program Orientation Week, Victoria
- Privacy Implications of the USA Patriot Act, Ontario OIPC Privacy and Security Conference, Toronto
- Privacy, Consent and Health Research Speech, Saskatchewan OIPC Health Privacy Conference, Regina
- Privacy Implications of the USA Patriot Act, US Consulate, Vancouver

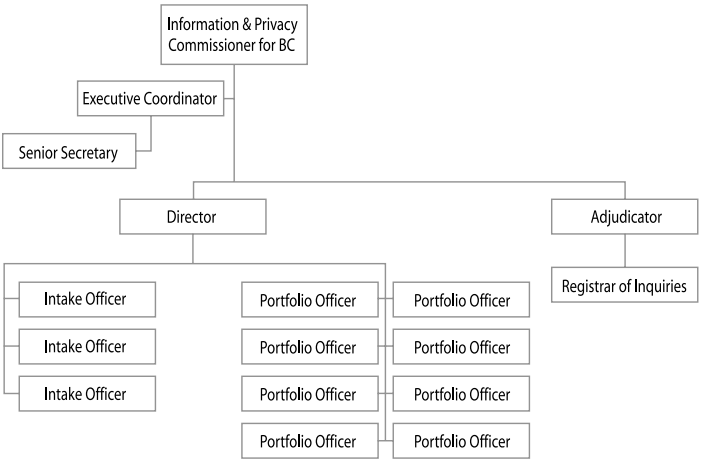
Personal Information Protection Act Presentations

- Canadian Life and Health Insurance Association Legal Section, Kelowna

- Greater Victoria Chamber of Commerce, Victoria
- BC & Yukon Building and Construction Trades Council, Victoria
- Canadian Public Sector Pension & Benefits Trustees Association, Vancouver
- Elder College, Capilano College, Vancouver
- University of Victoria Law Centre, Victoria
- M'akola Society, Victoria
- Canadian Bar Association, Vancouver
- Canadian Film and Television Production Association, Vancouver.

Organizational Chart

The OIPC has 17 full time staff, including the Commissioner. It is a very lean organization, as the following chart demonstrates:



Financial Reporting

As noted earlier, the Information and Privacy Commissioner is an independent officer of the Legislature who monitors and enforces compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). FIPPA applies to more than 2,200 public agencies, and accords access to information and protection of privacy rights to citizens. PIPA regulates the collection, use, access disclosure and retention of personal information by more than 300,000 private sector organizations. The Commissioner is also the Registrar under the *Lobbyist Registration Act*, which requires those lobbying certain public agencies to register and pay a fee.

Funding for the OIPC's operation is provided through a vote appropriation (Vote 5), as described below in note 3, and by recoveries for any OIPC-run conferences. All OIPC payments are made from, and funds are deposited in, the Province's Consolidated Revenue Fund.

Significant Accounting Policies

Consistant with generally accepted accounting principles in Canada, the OIPC's significant accounting policies are as follows:

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

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

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

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

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

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

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

- Computer hardware and software 3 years
- Furniture and equipment 5 years.

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.

		2005 (unaudited)		2004 (unaudited)
	Operating	Capital	Total	Total
Appropriations	$2,248,000	$20,000	$2,268,000	$2,279,000
Gross Funds Available	$2,248,000	$20,000	$2,268,000	$2,279,000
Operating Expenses	-$2,174,787	0	-$2,174,787	-$2,027,466
Capital Acquisitions	0	-$12,419	-$12,419	-$30,817
Unused Appropriations[12]	**$73,213**	**$7,581**	**$80,794**	**$220,717**

Employee Benefits and Leave Liability

Accumulated liability with respect to vacation and other leave entitlements due to employees of the OIPC amounted to $40,253.57 as at March 31, 2005. The OIPC has fully funded this amount by transferring funds to the Province's leave liability account to cover future payment of these entitlements.

Capital Assets

		2005 (unaudited)		2004 (unaudited)
	Cost	Accumulated Amortization	Net Book Value	Net Book Value
Computer Hardware and Software	$71,414	-$38,499	$32,915	$38,081
Furniture and Equipment	$3,582	-$3,582	$0	$358
	$74,996	**-$42,081**	**$32,915**	**$38,439**

Commitments

The OIPC has a leasehold commitment with the British Columbia Buildings Corporation for building occupancy costs. The current lease is under renewal negotiation. Payments for office space for fiscal 2005/06 are estimated at $125,821.

Pension and Retirement Benefits

The OIPC and its employees contribute to the Public Service Pension Plan ("Plan") in accordance with the *Public Sector Pension Plans Act*. The Plan is a multi-employer defined benefit plan and is available to substantially all of the OIPC's employees. On behalf of employers, the British Columbia Pension Corporation administers the Plan, including paying pension benefits to eligible employees. The most recent actuarial valuation (March 31, 2002) has determined the Plan is in a surplus position. Effective January 1, 2002, the Plan's management changed to a joint trusteeship whereby the management, risks and

12 The surplus recorded in the 2005 operating funds represents an unstaffed senior Portfolio Officer position, which will soon be staffed.

benefits are shared between the employees and employers.

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

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

Printed on Recycled Paper