THE OIPC'S ROLE AND MANDATE

The Office of the Information and Privacy Commissioner for British Columbia (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). PIPA, 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; and
- 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 PIPA;

- initiate investigations and audits to ensure compliance with PIPA if the Commissioner believes there are reasonable grounds that an organization is not complying, including issuing binding orders;
- inform the public about PIPA;
- conduct or commission research into anything affecting the achievement of the purposes of PIPA;
- comment on the privacy implications of programs, automated systems or data linkages proposed by organizations;
- authorize the collection of personal information from sources other than the individual to whom the personal information relates; and
- investigate and resolve complaints that a duty imposed by PIPA has not been performed, an extension of time has been improperly taken, a fee is unreasonable or a correction request has been refused without justification

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.

Freedom of Information and Protection of Privacy Act

Access to Government Information

British Columbia's *Freedom of Information and Protection of Privacy Act*[1] (FIPPA) came into force on October 4, 1993. Politicians from across the political spectrum had introduced 12 different access and privacy bills in the Legislative Assembly during the preceding seventeen years, but none had passed until 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 in 2005. 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.

[1] http://www.oipc.bc.ca/legislation/FIPPA/FIPPA-ACT(18MAY2006).pdf.

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*[2] 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 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….

Here in British Columbia, a 1991 law reform report by the BC Freedom of Information and Privacy Association put it this way:[3]

> 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.

Access to information 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. These other accountability mechanisms require access to information about what public institutions think, decide and do, and the costs and impact of decisions and actions. They also require knowledge about what governments know about their citizens.

Privacy Protection

One privacy expert has said this about the importance of privacy:[4]

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

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

[3] BC Freedom of Information & Privacy Association, Information Rights for British Columbia (FIPA, Vancouver: 1991).

[4] Simon Davies, *Big Brother: Britain's Web of Surveillance & the New Technological Order* (London: Pan, 1996).

> 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 FIPPA, 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 FIPPA, 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":[5]

> …[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 it." 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.

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 Euro-

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

pean 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 2004, leaders of the Asia Pacific Economic Cooperation organization, of which Canada is a member, endorsed the APEC Privacy Framework, which sets out privacy principles to guide privacy protection in member economies.

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

Private sector privacy laws first emerged in Canada with Quebec's enactment in 1994 of privacy rules for the private sector. 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 below.)

The Basic Rules of Public Sector Privacy

Under 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.

If a public body uses personal information to make a decision that directly affects the individual, it must retain an individual's personal information for a minimum of one year. 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.

Protection of Access and Privacy Rights through 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; and
- 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, including all municipalities and regional districts, universities, colleges and schools, health authorities, health boards and hospitals, and municipal police forces; and
- 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 undue delay in disclosure might prejudice the rights of the applicant", 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 – most requests for review to the OIPC 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. 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; and
- 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, and the OIPC's binding decisions, are completely independent of government and are impartial.

Personal Information Protection Act

Personal information held in the private sector obtained legal protection in British Columbia on January 1, 2004, when the P*ersonal Information Protection Act*[6] (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.

[6] http://www.oipc.bc.ca/legislation/PIPA/PIPA(2006).pdf.

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", and these terms are defined in PIPA.

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 email, business fax number and other business contact information. It also

does not include "work product information", which is information prepared by individuals or employees in the context of their work or business. The "work product" designation applies only form the perspective of the individual who created the record. One employee's work product may include personal information of another individual. For example, an employee performance report prepared by a management employee of a company would be work product information as it relates to that management employee, but the personal information about the employee being assessed would be the personal information of the other employee.

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