BILL 30 – 2006
MISCELLANEOUS STATUTES AMENDMENT ACT (NO.2) 2006

Summary of Amendments to the *Freedom of Information and Protection of Privacy Act*

In Brief

On May 15, 2006, amendments to the *Freedom of Information and Protection of Privacy Act* (FOIPP Act) were passed as part of the *Miscellaneous Statutes Amendment Act (No. 2) 2006*.

The bill received Royal Assent on May 18, 2006. All of the amendments came into effect upon Royal Assent except the amendment to section 33(1)(d), which will come into effect on January 1, 2007.

The full text of the bill is available at http://www.leg.bc.ca/38th2nd/3rd_read/gov30-3.htm.

The amendments to the FOIPP Act:

- Provide the Information and Privacy Commissioner with authority to grant time extensions to public bodies when unexpected circumstances occur that prevent them from responding to access requests on time;

- Provide clarity to public bodies that information that may harm their negotiating position can be protected from release when responding to a request for access to records;

- Permit limited and temporary trans-border access, storage and disclosure of personal information in special circumstances where it is necessary for system maintenance and trouble-shooting, or where an employee or service provider is travelling outside of Canada and needs immediate access to personal information;

- Ensure transparency for the uses of personal health information contained in health information banks created under the *Health Act* by requiring the publication of summaries on an online public directory; and,

- Facilitate the removal from the coverage of the FOIPP Act public bodies that no longer exist or no longer meet the criteria for coverage.

Questions and Answers

Section 10 – Extending the time limit for responding

There are two changes to section 10.

1. The first change gives the Information and Privacy Commissioner (Commissioner) the authority to permit a public body to extend the time period for responding to a request for access to records in any case where the Commissioner considers it is fair and reasonable to do so.

What is the purpose of this amendment?

Prior to this change, a public body could only take an extension of time to respond to an access request where one of the following three circumstances applied:

a) the applicant did not provide enough detail to identify the records;
b) the request involved a large number of records; or
c) consultation with a third party or another public body was necessary.

A public body could not extend the time period for responding to an access request for any other reason, no matter how compelling. The public body could not even ask for the Commissioner's permission to take an extension of time for any other reason.

What is the effect of this amendment?

The change allows the Commissioner to grant permission to a public body to take a time extension in any case where the Commissioner considers it fair and reasonable to do so.

It is important to note that this amendment does not provide the public body with additional authority to take a time extension. It only permits a public body to request permission from the Commissioner for additional time when unexpected circumstances arise that prevent the public body, despite its best intentions and efforts, from responding to an access request in time. For example, a public body may not be able to meet its timelines due to a service disruption, strike, lockout or natural disaster (such as the 2003 forest fires in Kelowna).

2. The second change to section 10 clarifies that an applicant has the right to ask the Commissioner to review a time extension taken by a public body only when the public body has taken the time extension under its own authority. An applicant cannot ask the Commissioner to review a time extension that was granted by the Commissioner.

What is the purpose of this amendment?

Prior to this amendment, section 10 did not distinguish between an applicant's right to request a review where the public body had taken a time extension under its own authority versus where the public body had taken a time extension with the Commissioner's permission. In either situation, the public body had to inform the applicant that he or she had the right to ask the Commissioner to review any time extension taken by a public body – even where the time extension was taken with the Commissioner's permission.

As a result, applicants sometimes asked the Commissioner to review his own decision.

What is the effect of this amendment?

An applicant may still ask the Commissioner to review a public body's decision to take a time extension to respond to an access request. However, it is now clear that an applicant may not ask for a review of a time extension permitted by the Commissioner.

Section 17 – Disclosure of information harmful to the financial or economic interests of a public body

The amendment to section 17 clarifies that information that may harm a public body's negotiating position can be protected from release in response to a request for access to records.

What is the purpose of this amendment?

Section 17 permits a public body responding to an access to information request to refuse to release information that could reasonably be expected to harm its financial or economic interests. As part of this, it provides an illustrative, non-exhaustive list of the types of information that might be considered for protection under this section, including information *about negotiations* carried on, by or for a public body or the government of British Columbia.

However, section 17 did not provide specific protection for information that might not be about negotiations but whose disclosure could still be harmful to a public body's *negotiating position*. For example, specific elements of a contract are not information "about negotiations" but release of this information could harm a public body's financial interests by harming its future negotiating position for other contracts. While it could be argued that such information might already be protected under section 17, further clarity was desirable.

What is the effect of this amendment?

The amendment simply provides certainty to public bodies by adding another example of the type of information that might be protected under this section. It is not intended to change the intent of this exception or the harms test that must be met before the information may be protected. Nor is it intended to affect freedom of information rights or diminish accountability and openness of government. A public body can still only decline to release information under this exception when there would be harm to its financial or economic interests.

Section 33.1 – Disclosure of personal information inside or outside Canada

There are three changes to section 33.1:

1. **Section 33.1(1)(d)** This amendment clarifies that disclosure of personal information under an "agreement" made under an enactment of British Columbia or Canada must be under a *written* agreement. This specific amendment does not come into force until January 1, 2007.

   What is the purpose of this amendment?

   Prior to this change, there was no requirement under this provision for an "agreement" to be in writing. Public bodies could, if they chose, share personal information under an informal or undefined verbal agreement.

   What is the effect of this amendment?

   Public bodies will have to ensure they have written agreements if they wish to continue to disclose personal information under an agreement pursuant to section 33.1(1)(d). To give public bodies time to enter into written agreements where they do not already exist, the effective date for this specific amendment is January 1, 2007.

2. **Sections 33.1(1)(e) and (e.1)** These changes will permit officers or employees of public bodies to access personal information while temporarily travelling outside Canada where that access is necessary for the performance of their duties. The changes will also allow a service provider of a public body that is authorized to access personal information to do so while temporarily travelling outside Canada where that access is normally necessary for the performance of duties in relation to the public body.

   What is the purpose of these amendments?

   Before these amendments, employees and service providers were prevented from using Personal Digital Assistants (e.g., a Blackberry or Palm Pilot) or laptops when travelling outside of Canada. This restriction presented

significant challenges for government and other public bodies since such devices are frequently and increasingly used by public employees to check e-mail or to share files remotely.

What is the effect of these amendments?

These changes will address the unintended consequence of preventing employees and service providers, in the performance of necessary duties, from using devices such as laptops or Personal Digital Assistants to check e-mail or share files remotely while temporarily travelling outside Canada.

In particular, Personal Digital Assistants and laptops enable public employees travelling outside of Canada as part of their jobs, to perform essential services that may require them to access remotely the personal information of their clients. For example, physicians travelling abroad may need to connect remotely to their hospital database to read reports about patients.

What does "temporarily travelling outside Canada" mean? Does it mean days, weeks, months?

"Temporarily travelling" is not defined as a specific time. It could be days if the employee is at a conference, it could be a week if the employee is on a business trip, and it might be a month if the employee is on an extended assignment abroad that necessitates remote access to government files. However, it does mean that it is not a permanent situation.

Can employees temporarily travelling to another country take personal information with them on portable devices such as laptops, memory sticks, disks, or Personal Digital Assistants?

Public bodies and service providers should consider the requirements of sections 33.1(1)(e) or (e.1) carefully, keeping in mind that disclosure of personal information outside Canada pursuant to these sections is only permitted if it is necessary. Public bodies should also note that section 30.1 allows storage of personal information outside Canada only, amongst other things, for the purpose of disclosure allowed under the FOIPP Act. Therefore, if a portable device contains personal information that does not meet the requirements of sections 33.1, then no authority exists for the disclosure or the storage of the personal information outside Canada, including on employees' portable devices.

Can public body employees travelling outside Canada who have administrative privileges for computer systems remotely connect to those computer systems using administrative access?

A public body employee who is temporarily travelling outside of Canada can only remotely access personal information contained in a public body's computer system if access to the specific personal information is necessary for the performance of his or her duties.

It seems unlikely that an employee with administrative privileges would be required to perform administrator type duties while out of the country. It is more likely that another employee within the public body who also has administrative privileges would be asked to perform such tasks.

It is important to note that these provisions are subject to a "necessary" test. The first preference is always to limit access to personal information to within Canada. Wherever possible, public bodies must avoid permitting access to personal information from outside Canada. But in some cases, the particular attention of a specific employee is necessary and where that employee happens to be out of the country at the time, the delivery of an essential service should not be impeded because of this absence.

If an employee is travelling in a foreign country and receives a demand from a foreign authority to disclose personal information, what should the employee do?

Under section 30.2 of the FOIPP Act, any foreign demand for the disclosure of personal information that is unauthorized by the FOIPP Act must be reported to the Minister responsible. The Ministry of Labour and Citizens' Services will assess the situation and involve the appropriate people including the public body responsible for the personal information and legal counsel if necessary.

3. **Section 33.1(1)(p)** This is a new provision permitting a public body or a service provider of a public body to disclose personal information where it is necessary for installing, implementing, maintaining, repairing, trouble shooting or upgrading electronic systems or equipment, or for data recovery following an electronic system failure. Disclosure of personal information outside of Canada is limited to temporary access and storage for the minimum time necessary, and in the case of data recovery, can only occur if there has been an actual system failure.

What is the purpose of this amendment?

Since restrictions on the trans-border flow of personal information were added to the FOIPP Act in 2004, public bodies have worked hard to negotiate or re-

negotiate contract terms that would require service providers to store and access personal information from within Canada only. In most circumstances, public bodies were able to negotiate creative terms, such as:

- setting up offices or servers in Canada;
- stripping or anonymizing personal information;
- using 'dummy data';
- using Canadian based subcontractors for maintenance; and,
- sending foreign-based personnel to Canada to service systems.

However, these strategies have not worked for all contracts. In some cases, only a handful of service providers in the world service a particular piece of electronic equipment and they are all located outside Canada. These service providers are not always willing or able to set up an office in Canada or send personnel to Canada in every case.

Public bodies are critically dependent on these services for the safe and efficient operation of essential and specialized equipment like MRI machines. These machines and a number of essential software applications must be maintained and repaired remotely. Prior to this amendment, public bodies had no options for dealing with malfunctioning equipment and systems which in many cases manage critical medical and security operations.

What is the effect of this amendment?

This provision will allow out-of-the-country system and equipment maintenance and data recovery to take place but under strict conditions: the out-of-country access must be necessary and the information can only be stored or accessed from outside Canada for the minimum time necessary to complete the task.

In addition, for data recovery purposes, the out-of-country service provider may only access and store relevant information after the system failure has occurred. The out-of-country service provider cannot store such data for preventative purposes in anticipation of a system failure.

Will this amendment allow public bodies to disclose personal information outside Canada for broad purposes and permit ongoing and permanent foreign access to and storage of personal information for "maintenance"?

Section 33.1(1)(p) will not allow the disclosure, storage and access to personal information from outside of Canada for any given purpose. It can be applied only in limited and specific controlled circumstances where disclosure and the temporary access to and storage of personal information outside

Canada is necessary for electronic system or equipment maintenance or for data recovery – and only for the minimum time necessary.

Prior to choosing this option, public bodies should implement an escalation strategy to consider alternatives for system maintenance and repair that do not require disclosure, storage or access to personal information outside of Canada. For example, a public body could consider:

1. Attempting to resolve the issue by telephone or email first without the need to disclose or permit access to personal information;
2. Sending a test database with 'dummy data' outside of Canada instead of the actual database;
3. Anonymizing or stripping personal identifiers before disclosing or permitting access to personal information;
4. Asking the service provider to train public body personnel to perform system maintenance within Canada;
5. Asking the service provider to use Canadian-based subcontractors for system maintenance purposes; or,
6. Determining whether it is feasible for the service provider to send personnel to Canada to resolve the issue.

Where foreign access and storage is permitted, it must be under tightly controlled and secure circumstances. Public bodies and their service providers are required to make reasonable security arrangements when handling personal information to protect it from unauthorized access and disclosure.

What does "temporary" mean?

Section 33.1(1)(p)(ii)(A) makes it clear that "temporary" means for the "minimum time necessary".

Section 69.1 – Public information regarding health information banks

Health care bodies are required to publish on the B.C. Government's online Personal Information Directory summaries that explain the content and purpose of health information banks and related information sharing agreements. A health information bank is a database containing personal health information that has been designated or established by an order of the Minister of Health under the *Health Act*.

This is a new section that complements new provisions for health information banks in the *Health Act*.

What is the purpose of this amendment?

Publishing this information on the Personal Information Directory will increase openness and transparency by providing the public with information about health information banks. The public will be able to search the online directory for information on who is responsible for administering the health information bank, the specific health information stored in the bank, how it is used, and to whom it is disclosed.

What is the effect of this amendment?

Health care bodies will be required to publish and maintain, on the government's Personal Information Directory, summaries explaining the content and purpose of health information banks and related information sharing agreements. As well, the Ministry of Health will be required to conduct privacy impact assessments of its health information banks and related health information sharing agreements.

Section 76.1 – Ministerial regulation making power

This amendment provides the Minister responsible for the FOIPP Act with regulation-making power to remove from coverage of the FOIPP Act certain types of public bodies that no longer exist or that no longer meet the criteria for coverage set out by the legislation. These public bodies are listed in schedules to the FOIPP Act and include agencies, boards, commissions, corporations, offices, or other bodies, as well as governing bodies of professions or occupations.

What is the purpose of this amendment?

Prior to this amendment, the Minister already had the authority, by regulation, to add a public body to the coverage of the FOIPP Act or to designate (or change the designation of) the head of a public body. However, the Minister had no authority to remove a public body by regulation; they could be removed only by legislative amendment.

As a result of this inconsistency, the schedules listing the public bodies were up-to-date with respect to new public bodies added to the FOIPP Act but out-of-date with respect to public bodies to be removed. Additionally, where a public body underwent a name change, the new name was added but the old name was not removed.

What is the effect of this amendment?

Permitting the on-going removal of defunct public bodies by Ministerial Regulation will ensure that the public body schedules are kept up-to-date, removing the confusion that currently exists where defunct bodies are listed or

where public bodies are listed twice by different names. It will also expedite the process for removing public bodies by providing a simpler non-legislative solution for updating the lists of public bodies covered by the FOIPP Act.

It is important to note that the regulation making power will only apply to the removal of public bodies for two reasons: (a) the public body no longer exists; or, (b) it no longer meets the criteria for coverage by the FOIPP Act. A legislative amendment will still be necessary to remove a public body for any other reason.

Those public bodies that are removed from the FOIPP Act will be listed on a publicly accessible website to ensure accountability and transparency.