

# Health Law Bulletin

## Developments under the *Freedom of Information and Protection of Privacy Act for Public Bodies*

On October 7, 2004, the BC government introduced Bill 73, the *Freedom of Information and Protection of Privacy Amendment Act* (“Bill 73” or the “Bill”). The Bill was enacted following concerns about the impact of the *USA Patriot Act* (the “*Patriot Act*”) on the privacy rights of BC residents. Its purpose is to restrict the ability of foreign government officials to access the personal information of BC residents, and it creates a number of new obligations for public or government bodies and the service providers with whom these bodies contract. The Bill received Royal Assent on October 21, 2004 and came into force on the same date.

Bill 73 makes some fundamental changes to the *Freedom of Information and Protection of Privacy Act* (“*FOIPPA*” or the “*Act*”) and its application to public bodies. The most significant of these changes are: (1) the application of *FOIPPA* obligations to private sector businesses that provide services under contract to public bodies; (2) the creation of restrictions on the transfer of personal information across international boundaries; and (3) the imposition of new and more stringent sanctions for non-compliance with *FOIPPA* by service providers, or their employees and/or associates.

This Bulletin seeks to briefly summarize the purpose and effect of Bill 73 and the steps public bodies need to follow in order to ensure their compliance with the

Bill. It also discusses in further detail two reports issued on October 29, 2004 by the British Columbia Information and Privacy Commissioner (the “Commissioner”) which explore in detail the efficacy of Bill 73, and report on the obligations of public bodies in respect of outsourcing initiatives with contractors based in the United States and other jurisdictions.

### ***BACKGROUND AND PURPOSES OF BILL 73***

The initial impetus for the Bill was the ***Patriot Act***, a piece of legislation introduced by the American government in response to the terrorist attacks in the United States on September 11, 2001. Since the ***Patriot Act*** was enacted, it has been the subject of a great deal of criticism both in the United States and abroad because of the sweeping powers it grants to American authorities to access personal information.<sup>1</sup>

The concern among Canadians has been that the ***Patriot Act*** is not limited in scope to United States residents. Many Canadian groups have raised concerns that the ***Patriot Act*** would enable American authorities to access personal information about BC residents as a result of Canadian-U.S. partnerships and, in particular, outsourcing contracts that government bodies may enter into with U.S.-linked service providers. Personal information about British Columbians that is physically stored in the United States might, for example, be subject to a disclosure order under the ***Patriot Act***. Likewise, some have speculated that even information stored in Canada might be subject to a production order issued to a U.S.-linked service provider who had access to the information through a Canadian subsidiary. This debate has raised questions as to how well the ***Act*** protects against such disclosure. Bill 73 was designed, in part, to address these issues.

In response to public concern, the Commissioner announced on May 28, 2004 the commencement of an investigation into

the privacy implications of outsourced public services involving U.S.-linked private sector companies. The British Columbia government, in August of this year, also announced its intention to release new legislation to combat the effects of the ***Patriot Act*** on outsourcing by public bodies in British Columbia. Bill 73 is that legislation.

### ***BILL 73 – FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY AMENDMENT ACT***

The key provisions of Bill 73 can be summarized as follows:

- ***Personal Information.*** The Bill amends the definition of “personal information” to exclude a person’s contact information. The definition of personal information now includes “***all recorded information about an identifiable individual other than contact information***”.<sup>2</sup>
- ***Application of Disclosure Rules.*** Perhaps the most fundamental change introduced by Bill 73 is that it amends the ***Act*** so that restrictions on the use, disclosure, collection and storage of personal information expressly apply, not only to public bodies, but also to their service providers. In particular, restrictions on the disclosure of personal information are extended to all employees, officers, directors of public bodies, as well as to all employees, affiliates and associates of service providers under contract with public bodies. These changes have extended accountability under the ***Act*** into the private sector.
- ***Storage of Personal Information in Canada.*** Bill 73 requires that personal information under the custody or control of a public body must be stored in Canada and must only be “***accessed in Canada***”. While the Bill allows for certain exceptions, personal information stored by a service provider must not be made accessible to its parent company in the United States. Public bodies are also restricted in their ability to

conduct business with service providers based in a foreign jurisdiction where that business involves transborder transfers of personal information. Of course, individuals may still consent to the storage of their personal information in another jurisdiction. And, if **FOIPPA** otherwise authorizes the disclosure of information outside of Canada, it may be permissible for that information to be stored in the United States.

- **Reporting Obligations.** A public body, an employee of that public body, or an employee or associate of a service provider who receives a foreign demand for disclosure that is not authorized by the **Act**, or who knows or suspects that a request for disclosure is for the purpose of responding to a foreign demand for disclosure, must immediately notify the Minister of Management Services.
- **Whistle Blower Protections.** The Bill also contains whistle blower protections for employees of public bodies or service providers who report a foreign demand for information. Employers must not discipline or otherwise disadvantage an employee who complies with **FOIPPA** or who has reported a contravention of the **Act**.
- **No Unauthorized Disclosure.** Bill 73 specifically prohibits public bodies (and their employees, officers and directors) or service providers (and their employees or associates) who have access (whether or not such access is authorized) to personal information that is in the custody or control of a public body from disclosing the information, except as authorized by the **Act**.
- **Non-Compliance.** The Bill makes it an offence to make unauthorized disclosure of personal information in the custody or control of a public body. It is also an offence to store personal information outside of

Canada or allow access to such information from outside Canada, to fail to report a foreign demand for disclosure, or to breach the whistle-blower protections of the **Act**. Persons committing an offence could be liable to a fine ranging from \$2,000 to \$500,000. In prosecution of an offence under this section, it is a defence to prove that the person charged exercised due diligence to avoid the commission of the offence.<sup>3</sup>

- **Authorized and Unauthorized Disclosures.** The **Act** previously did not make a distinction between disclosure inside and outside of Canada. The **Act** now provides separate bases on which personal information under the custody or control of a public body may be disclosed within and outside of Canada. For example, the **Act** previously provided that disclosures are permissible if made for “**the purpose for which [personal information] was obtained or compiled or for a use consistent with that purpose**”. It now provides that such disclosures can be made only so long as the disclosure takes place within Canada. Likewise, disclosure was permissible “**for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information**”, but that authority is now limited by a requirement that disclosure only be made if it is to a domestic court or tribunal.
- **Effective Date.**
  - (a) For contracts to which the government or a ministry is a party, the new disclosure rules outlined in Bill 73 apply to all contracts for which the contract commitment date is later than October 12, 2004. For contracts entered into by other public bodies, the new rules apply if the contract commitment date of the contract is later than October 21, 2004 (the date on which the Bill received Royal Assent). “Contract commitment date” is a defined

term and means (i) in the case of a contract that a public authority is legally obliged to enter into as a result of a completed binding competitive process, the date on which the process was completed, or (ii) in any other case, the date on which the contract was entered into by the public authority.

(b) Public authorities who are parties to contracts for which the contract commitment date was earlier than the foregoing dates are subject to the previous disclosure rules under the **FOIPPA** until the end of the initial term of the contract. The new rules are applicable upon renewal. In the meantime, such public authorities must use all reasonable efforts to come into compliance with the new disclosure rules as soon as reasonably possible.

#### ***HOW CAN PUBLIC BODIES ENSURE COMPLIANCE WITH BILL 73?***

To ensure compliance with Bill 73, we recommend that public bodies take steps to review the contracts they may have with (a) private service-providers and (b) other public bodies or governments, as well as the process they have in place for entering into such contracts. For example, it would be prudent to:

- Review contracts with a commitment date after October 21, 2004 and:
  - (i) advise the other party(s) to the contract (whether private service provider(s) or other public authorities) that the new disclosure rules apply, and
  - (ii) prepare an amendment (“Privacy Amendment”) to such contract(s) which requires the other contracting party(s) to comply with the new disclosure rules and to require their employees or associates to so comply;
- Review contracts with government/ministries whose commitment date is after October 12, 2004 and propose a Privacy Amendment to such contract(s) which requires the other contracting party(s) to comply with the new

disclosure rules and effectively allocates responsibility between the parties regarding costs and liabilities for compliance with and breach of the new disclosure rules;

- Review any contracts currently under negotiation with private service providers (or with public bodies or government) to ensure Privacy Amendment provisions are included in the final form of contract;
- Advise employees of their obligations under the **Act**. In particular, notify employees of their duties to not disclose personal information except as authorized under the **Act** and to report any requests for disclosure of information that they suspect are in relation to a foreign demand for disclosure. To ensure compliance, it would also be advisable to notify employees of the consequences of a failure to comply with these obligations;
- Review existing (or develop new) internal policies and guidelines addressing outsourcing contracts, and include new provisions regarding assurance that Privacy Amendment protections are part of the protocols;
- Review existing privacy policies to determine whether adequate steps are being taken to guard against unauthorized disclosure; and
- Public bodies may also wish to review the Provincial Government’s “Privacy Protection Measures” which can be found at [www.mser.gov.bc.ca/FOI\\_POP/main/contracting.htm](http://www.mser.gov.bc.ca/FOI_POP/main/contracting.htm).

#### ***WILL THE PRIVACY COMMISSIONER’S INVESTIGATION IMPACT ON COMPLIANCE WITH FOIPPA AND BILL 73?***

Between May and September 2004, the Commissioner conducted an investigation into a proposed outsourcing of health information by the provincial government to U.S.-based service providers. In that context, the Commissioner

issued a call for submissions on the implications of public sector outsourcing and the *Patriot Act*. The Commissioner reportedly received some 500 responses from within British Columbia and across Canada, the United States and Europe. The Commissioner's report (the "Report"), released October 29, 2004, reflects a public concern for a variety of issues related to the sharing of personal information across international boundaries. The Commissioner's conclusions as they apply to public bodies are discussed in more detail below.

#### *WHAT SECURITY MEASURES SHOULD PUBLIC BODIES HAVE IN PLACE?*

Ultimately, the Report concludes the outsourcing of public body functions to private contractors is not inconsistent with the *FOIPPA*, and no outright ban on outsourcing initiatives is mandated by the *Act*. However, the Commissioner does conclude that outsourcing initiatives with U.S.-linked service providers do pose a potential risk of disclosure under the *Patriot Act*. The need for legislative change as well as legal and practical safeguards to prevent such disclosures is therefore necessary.

Section 30 of the *Act* provides that:

The head of a public body must protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposals....

Section 30, the Commissioner says, requires that public bodies take steps to ensure that reasonable security arrangements are made to protect against unauthorized disclosure of information disclosed to, or generated by, US-linked contractors. The Report sets out the following

guidelines on what will be considered reasonable:

- A public body, by contracting out the provision of services to a private sector body, will not relieve itself of its obligations to protect personal information.
- "Reasonable" security measures are required, "not infallible" ones. "Section 30 requires reasonable, but not absolute, security."
- What will be considered "reasonable" security, within the meaning of section 30, will depend on the nature of the personal information involved and the consequences of its unauthorized disclosure.
- Security arrangements to protect against unauthorized disclosure will always be necessary, regardless of the relative sensitivity of the personal information.

The Report concludes that public bodies must always take reasonable steps to protect privacy, but that what is required is flexible and will vary from case to case. The Commissioner has not commented on the Province of British Columbia Privacy Protection Measures, but these may provide some additional guidance to public bodies in ascertaining whether their own security measures are adequate. The Commissioner's recommendations, summarized in the attached Appendix, also provide some further guidance to public bodies.

Whether these recommendations will be legislatively implemented is yet to be determined. However, public bodies can take some practical suggestions from the Commissioner's recommendations such as: (1) building credit mechanisms into contracts with service providers; (2) conducting regular and thorough audits of a contractor's performance; (3) regular review of practical and legal security measures; and (4) reviewing the scope, extent and necessity for information-sharing agreements.

## THE COMMISSIONER'S COMMENTS ON BILL 73

Simultaneously with the Report, the Commissioner issued his comments on Bill 73 in the form of a letter to the BC government. While acknowledging that the Bill was a useful step in protecting personal information, the Commissioner urged the BC government to consider further amendments, including:

- **Transitional Provisions.** The prohibitions against the storage of personal information outside Canada should apply retrospectively to all existing contracts between public bodies and service providers.
- **Prohibition Against Foreign Disclosure.** The BC government should enact an express prohibition against the disclosure of personal information in response to a foreign demand for disclosure, including a foreign court order. While the Bill contains a provision along these lines, the Commissioner says the prohibition should be clarified and strengthened.
- **Authorized Disclosure Inside or Outside Canada.** The Commissioner argues that those sections in Bill 73 addressing the purposes for which personal information may be disclosed outside of Canada need clarification so that they do not receive too broad an interpretation.
- **Information Sharing Agreements.** The Commissioner asserts that the potential breadth of information sharing agreements is problematic given the absence of meaningful standards by which to assess such agreements. Thus, the BC government should (after completing an audit of information sharing agreements as recommended by the Report) consider amending the **FOIPPA** to set stricter standards for information sharing agreements.
- **Penalties for Unauthorized Disclosure.** The Commissioner says the fine thresholds imposed in the Bill should be in the range of \$1,000,000, and no

distinction should be made between individuals, corporations or partnerships that are service providers. Additionally, imprisonment should also be available as punishment for non-compliance.

The Commissioner's comments on Bill 73 provide a useful critique of the new legislation. However, while they may foreshadow still further changes to **FOIPPA**, they do not alter the legal authority or effect of Bill 73.

## SUMMARY

Bill 73 will have a significant impact on all public bodies governed by the **FOIPPA** as well as the service providers with whom the public bodies contract. A copy of the Bill can be located at [http://www.legis.gov.bc.ca/37th5th/3rd\\_read/gov73-3.htm](http://www.legis.gov.bc.ca/37th5th/3rd_read/gov73-3.htm). Additionally, you can access the Commissioner's web site at <http://www.oipcbc.org> for further information about the Report. Should you wish to revise your contracts as suggested above, please feel free to contact us. For further assistance in understanding these new disclosure rules and in ensuring compliance, please contact our Health Law Practice Group.

## (Footnotes)

- <sup>1</sup> The Patriot Act, for example, (1) Permits FBI officials to compel the disclosure of "any tangible thing", including personal information, without first establishing probable cause or even reasonable grounds as a basis for obtaining the information; (2) To obtain a disclosure order, officials must satisfy the court only that the information is sought in connection with an anti-terrorism investigation; and (3) Prohibits an entity from to advise a person that their personal information has been seized.
- <sup>2</sup> "Contact information" is defined as information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business e-mail or business fax number of the individual.
- <sup>3</sup> It remains to be seen how these offence provisions will be read in conjunction with s. 73 of the Act which protects public bodies who make disclosure in good faith from civil liability.

## APPENDIX:

### The Commissioner's Recommendations

The Report provides sixteen recommendations made to the government of British Columbia, the government of Canada and to public bodies within British Columbia. Below, we have summarized those recommendations that are most relevant to the newly enacted Bill 73 and to public bodies and their information practices.

**Recommendation 1** - The Commissioner has recommended that the British Columbia government enact amendments to **FOIPPA** similar to those appearing in Bill 73, including amendments which, among other things: (1) would prohibit any personal information from being sent outside Canada (whether for management, storage or safekeeping) and from being accessed outside of Canada; (2) impose direct responsibilities on contractors to public bodies to ensure compliance with the **FOIPPA**; (3) require contractors to notify public bodies of any subpoena, warrant, order or demand for disclosure of personal information made by a foreign court or authority; (4) provide the Commissioner with the authority to investigate contractors' compliance with the **FOIPPA**; and (5) Make it a provincial offence for a public body or its contractors to use or disclosure personal information or to send it outside of Canada in contravention of the **FOIPPA**.

**Recommendation 4** - The Commissioner also recommends that all public bodies governed by the **FOIPPA** ensure that they commit, for the duration of all relevant contracts, the financial and other resources necessary to monitor contract performance and punish

breaches, as well as to detect and defend against actual or potential disclosure to a foreign court or authority.

**Recommendation 5** - The Commissioner argues that it is not sufficient for public bodies to trust that its contractors will self-report their breaches of the **Act** and/or governing contracts. He recommended that public bodies implement a program of regular and thorough compliance audits to be performed by a third party auditor that has the necessary expertise to perform the audit and recommend necessary changes. The Commissioner goes on to suggest that contracts may even provide that the contractor will pay for any audits that uncover material non-compliance with the contract.

**Recommendations 9, 10 and 12** - The Commissioner has called for the British Columbia government to undertake a comprehensive review of all interprovincial, national and trans-national information sharing agreements affecting public bodies in British Columbia and all data mining efforts by all public bodies in British Columbia. The Commissioner recommends that the provincial government ensure that, within 60 days of the report, all ministries are fully compliant with section 69 of the **FOIPPA**, which requires ministries to maintain and publish a personal information directory to provide information about records held by that ministry, and about the use of those records by ministries of the government of British Columbia. He also recommends that the reporting requirements in section 69 be applied to all other public bodies.

# DAVIS LEGAL ADVISORS since 1892 & company

## Health Law Group

Members of Davis & Company's Health Law Group have a wide range of experience in providing legal services in the health-care field. We have acted on behalf of both public and private sector health-care clients on matters involving government relations, administrative and regulatory controls; corporate governance; professional negligence; patient rights; employment law and freedom of information and protection of privacy issues.

We also have an extensive commercial practice involving health-care clientele. In this connection, we provide general corporate/commercial advice, as well as assistance on taxation and real estate issues.

For more information about this bulletin, please call Linda Parsons, Suzanne Kennedy or Kate Bake-Paterson.

**Linda Parsons**  
Chair, Health Law Group  
Vancouver  
604.643.6445  
linda\_parsons@davis.ca

**Suzanne Kennedy**  
Health Law Group, Vancouver  
604.643.6470  
skennedy@davis.ca

**Kate Bake-Paterson**  
Health Law Group, Vancouver  
604.643.6375  
kbakepaterson@davis.ca

This bulletin is intended to provide our general comments on developments in the law. It is not intended to be a comprehensive review nor is it intended to provide legal advice. Readers should not act on information in the bulletin without seeking specific advice on the particular matter. The firm will be pleased to provide additional details or discuss how this information is relevant to a specific situation.

**VANCOUVER**  
2800 Park Place  
666 Burrard Street  
Vancouver, British Columbia  
Canada V6C 2Z7  
Tel 604.687.9444  
Fax 604.687.1612

**TORONTO**  
1 First Canadian Place  
Suite 5600, PO Box 367  
100 King Street West  
Toronto, Ontario  
Canada M5X 1E2  
Tel 416.365.3500  
Fax 416.365.7886

**MONTRÉAL**  
1010 de la Gauchetière Street West  
Suite 2250, Place du Canada  
Montréal, Québec  
Canada H3B 2N2  
Tel 514.392.1991  
Fax 514.392.1999

**CALGARY**  
3000 Shell Centre  
400 - 4th Avenue SW  
Calgary, Alberta  
Canada T2P 0J4  
Tel 403.296.4470  
Fax 403.296.4474

**EDMONTON**  
1201 Scotia Tower 2  
10060 Jasper Avenue  
Edmonton, Alberta  
Canada T5J 4E5  
Tel 780.426.5330  
Fax 780.428.1066

**WHITEHORSE**  
Suite 200  
304 Jarvis Street  
Whitehorse, Yukon  
Canada Y1A 2H2  
Tel 867.393.5100  
Fax 867.667.2669

**YELLOWKNIFE**  
Suite 802 Northwest Tower  
5201 - 50th Avenue  
Yellowknife, NWT  
Canada X1A 3S9  
Tel 867.669.8400  
Fax 867.669.8420

**TOKYO**  
Kasumigaseki Building, 31st Floor  
2-5, Kasumigaseki 3-Chome  
Chiyoda-ku, Tokyo  
100-6031, Japan  
Tel 81.3.5251.5071  
Fax 81.3.5251.5072

[www.davis.ca](http://www.davis.ca)