



Request for Submissions

Assessing USA Patriot Act Implications for Privacy Compliance under British Columbia's Freedom of Information and Protection of Privacy Act

May 28, 2004

1.0 INTRODUCTION

There is significant and pressing interest and public concern about privacy implications of the USA Patriot Act¹ for British Columbians' personal information involved in the outsourcing of public services to US-linked private sector service providers. The issue has received widespread media coverage in British Columbia and across Canada since February. Government, the media, interest groups and members of the public have made requests for both general and situation-specific guidance or oversight by the Information and Privacy Commissioner respecting the implications of the USA Patriot Act for public body compliance with the *Freedom of Information and Protection of Privacy Act* ("FOIPP Act").

Following the process described below, I intend to examine issues related to the USA Patriot Act and British Columbians' personal information involved in the outsourcing of public services to US-linked private sector service providers. I welcome input from government, interest groups, businesses and members of the public. This request for submissions does three things in relation to this process:

1. It describes the background to issues surrounding the USA Patriot Act and British Columbians' personal information involved in the outsourcing of public services to US-linked private sector service providers.
2. It sets out two questions I propose to address in relation to the USA Patriot Act and British Columbians' personal information involved in the outsourcing of public services to US-linked private sector service providers.
3. It describes the process I will follow in receiving input, examining the questions set out below and communicating the results of this work.

¹ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, Public Law 107-56 ("USA Patriot Act")

The process I am now initiating is intended to be flexible, consultative and as transparent as possible, including as to public availability of the submissions that are made to me. It will result in publication of an advisory letter or report.

The process is not directed at specific existing, proposed or contingent outsourcing projects or arrangements. The resulting advisory letter or report will not be binding or determine rights. .

2.0 BACKGROUND

Section 30 of the FOIPP Act requires every public body in British Columbia to protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Concerned parties have complained to my office that outsourcing contracts that give USA-linked companies access to personal information in the custody or under the control of public bodies in British Columbia violate section 30 of the FOIPP Act because of the reach and effect of the USA Patriot Act.

The USA Patriot Act is a United States federal law passed by the US Congress in the autumn of 2001, shortly after the terrorist attacks of September 11, 2001. President Bush signed it into law on October 26, 2001.

Concerned parties have complained that all USA companies and their affiliates are subject to the USA Patriot Act and, as such:

1. USA-linked private sector service providers may be required to disclose to the US Federal Bureau of Investigation personal information to which the service providers are given access in outsourcing arrangements with public bodies in British Columbia.
2. If a USA-linked private sector service provider is ordered to produce personal information pursuant to the USA Patriot Act, it is prohibited from disclosing the existence of that order.

To date, the only legal opinion available to the public or my office regarding the USA Patriot Act and outsourcing initiatives by British Columbia public bodies is by Jameel Jaffer, a lawyer with the American Civil Liberties Union (“ACLU”) in New York. The opinion is found in a February 23, 2004 affidavit sworn by Jaffer in support of a British Columbia Government & Services Employees’ Union (“BCGEU”) court challenge to proposed outsourcing of functions connected with the administration of

British Columbia’s Medical Services Plan (“MSP”).² MSP is British Columbia’s public health insurance plan, which is administered under the *Medicare Protection Act*. The BCGEU court challenge focuses on section 215 of the USA Patriot Act (the text of section 215 is found in Appendix 1 to this request for submissions). Jaffer’s opinion addresses the following two questions:

1. How does the USA Patriot Act (“the Act”) affect the confidentiality of personal information, including personal health information, held by, in possession of, or which can be accessed by a corporation which is subject to the Act?
2. If a subsidiary of a U.S. company has possession of, or access to health or other personal information of Canadian residents, will that information be subject to disclosure under the USA Patriot Act.

Jaffer’s opinion is that several USA Patriot Act provisions “directly or indirectly expand the government’s authority to obtain personal information held by entities in the United States” (p. 1). The opinion then refers specifically to three examples, sections 215, 218 and 505.

Jaffer’s opinion is that section 218 of the USA Patriot Act “expands the [US federal] government’s authority to conduct secret searches” (p. 1):

Section 218 of the Act expands the government’s authority to conduct secret searches without meeting the ordinary “probable cause” requirement. Ordinarily, the Fourth Amendment to the United States Constitution prohibits the government from conducting searches without first showing “probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offence.” *See, e.g., Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal quotation marks omitted). Section 218 allows the government to conduct searches in certain criminal investigations without meeting this standard.

As regards section 505, Jaffer’s opinion reads as follows (p. 1):

Section 505 of the Act expands the government’s “National Security Letter” authority – an authority that allows the FBI unilaterally to order certain kinds of organizations to turn over financial, credit, and electronic communications records. A gag provision prohibits anyone served with a National Security Letter from speaking about the letter to anyone else.

Jaffer’s opinion describes section 215 of the USA Patriot Act as the provision “that poses the most direct threat to the privacy of records relating to personal health” (p. 1). Because of its length, Jaffer’s opinion about section 215 is reproduced in Appendix 2 to this request for submissions.

² *British Columbia Government & Services Employees’ Union* (petitioner) v. *The Minister of Health Services & The Medical Services Commission* (respondents), British Columbia Supreme Court, Victoria Registry No. 04-0879.

As noted above, Jameel Jaffer's opinion addresses only three sections of the USA Patriot Act. While those sections appear to be the provisions most worth considering, I will not restrict my examination of the questions raised below to sections 215, 218 and 505 if other provisions of the USA Patriot Act are also pertinent.

3.0 ISSUES

I intend to examine issues related to the USA Patriot Act and British Columbians' personal information involved in the outsourcing of public services to US-linked private sector service providers by addressing these questions:

1. Does the USA Patriot Act permit USA authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of USA-linked private sector service providers? If it does, under what conditions can this occur?
2. If it does, what are the implications for public body compliance with the personal privacy protections in the FOIPP Act? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with the FOIPP Act?

4.0 INVITATION FOR INPUT

I will do my work using the following process:

1. I will accept submissions on the questions set out above from all quarters, including government, public bodies, businesses, labour groups, interest groups and the general public. I will also welcome any input other Canadian privacy commissioners might wish to offer. Submissions must be in writing. I will not receive submissions orally and no public forums or sessions will be held.
2. Any submission must be clearly labelled "**Submission on the USA Patriot Act**" and must be delivered, mailed, faxed or e-mailed as follows:

Delivery:

2nd Floor, 756 Fort Street
Victoria, B.C. V8W 1H2

Mail:

P.O. Box 9038, Stn. Prov. Govt
Victoria, B.C. V8W 9A4

Fax:

(250) 387-1696

E-mail: info@oipc.bc.ca

3. The deadline for receipt of submissions in my office is **Friday, July 23, 2004, at 12:00 p.m. Victoria time**. My office takes no responsibility for the lateness of any submissions, including due to equipment or network failure.
4. Submissions will be made available for public review on my office's website, www.oipc.bc.ca.
5. In light of the submissions received, I may, as I consider necessary or desirable, seek or permit further input from any one or more of those who make submissions to me.
6. I will review all submissions, research the questions set out above and, as soon as is reasonably practicable, release a public advisory giving such reasoned and practical commentary and solutions as can be identified. My goal is to release the advisory before August 13, 2004 if feasible.

David Loukidelis
Information and Privacy Commissioner
for British Columbia

Appendix 1

Selected USA Patriot Act Provisions

The USA Patriot Act provisions to date brought to the attention of the Office of the Information and Privacy Commissioner are set out below.

1. SECTION 215, USA PATRIOT ACT

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the *Foreign Intelligence Surveillance Act of 1978* (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

- (a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.
- (2) An investigation conducted under this section shall--
 - (A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and
 - (B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.
- (b) Each application under this section--
 - (1) shall be made to--
 - (A) a judge of the court established by section 103(a); or
 - (B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and
 - (2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.

- (c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.
- (2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).
 - (d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.
 - (e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

SEC. 502. CONGRESSIONAL OVERSIGHT.

- (a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.
- (b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--
 - (1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and
 - (2) the total number of such orders either granted, modified, or denied.'

2. SECTION 218, USA PATRIOT ACT

SEC. 218. FOREIGN INTELLIGENCE INFORMATION.

Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the *Foreign Intelligence Surveillance Act of 1978* are each amended by striking “the purpose” and inserting “a significant purpose”

3. SECTION 505, USA PATRIOT ACT

SEC. 505. MISCELLANEOUS NATIONAL SECURITY AUTHORITIES.

- (a) **TELEPHONE TOLL AND TRANSACTIONAL RECORDS** - Section 2709(b) of title 18, United States Code, is amended--
 - (1) in the matter preceding paragraph (1), by inserting “at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director” after “Assistant Director”;

- (2) in paragraph (1)--
 - (A) by striking “in a position not lower than Deputy Assistant Director”; and
 - (B) by striking “made that” and all that follows and inserting the following: “made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and”; and

- (3) in paragraph (2)--
 - (A) by striking “in a position not lower than Deputy Assistant Director”; and
 - (B) by striking “made that” and all that follows and inserting the following: “made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”.

- (b) **FINANCIAL RECORDS** - Section 1114(a)(5)(A) of the *Right to Financial Privacy Act of 1978* (12 U.S.C. 3414(a)(5)(A)) is amended--
 - (1) by inserting “in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director” after “designee”; and
 - (2) by striking “sought” and all that follows and inserting ”sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”

- (c) **CONSUMER REPORTS** - Section 624 of the *Fair Credit Reporting Act* (15 U.S.C. 1681u) is amended--
 - (1) in subsection (a)--
 - (A) by inserting ”in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director” after “designee” the first place it appears; and
 - (B) by striking “in writing that” and all that follows through the end and inserting the following: ”in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted

- solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”;
- (2) in subsection (b)--
 - (A) by inserting “in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director” after “designee” the first place it appears; and
 - (B) by striking “in writing that” and all that follows through the end and inserting the following: “in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”; and

 - (3) in subsection (c)--
 - (A) by inserting “in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director” after “designee of the Director”; and
 - (B) by striking “in camera that” and all that follows through “States.” and inserting the following: “in camera that the consumer report is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”.

Appendix 2

The following is the text of Jameel Jaffer's opinion regarding section 215 of the USA Patriot Act:

In my view, Section 215 seriously compromises the confidentiality of a vast array of personal records in the custody or control of entities in the United States. I reach this conclusion for three reasons.

First, Section 215—unlike its predecessor provision, which could be used only against certain types of businesses—can be used against *any* person, business, or organization. Section 215 can be used, for example, against hospitals, schools, Internet service providers, libraries, or political organizations. At a hearing before the House Judiciary Committee on June 5, 2003, Attorney General John Ashcroft acknowledged that the FBI could use Section 215 to obtain bookstore purchase records, library circulation records, computer files, and even genetic information. *See* Hearing of the House Judiciary Committee, June 5, 2003 (testimony of Attorney General John Ashcroft), available at www.Janerights.org/ashcroft060503.htm. There is no doubt that the FBI could use Section 215 to force the disclosure of medical records and other records relating to personal health.

Second, Section 215—unlike its predecessor provision, which reached only records pertaining to suspected spies and terrorists—does *not* include an individualized suspicion requirement. One consequence is that the FBI can use Section 215 to order the disclosure of a particular person's records even if it has no reason to believe that the person is a spy, terrorist, or engaged in criminal activity of any sort. A second (related) consequence is that the FBI can use Section 215 to obtain entire databases implicating the privacy of hundreds or even thousands of people. If the FBI can specify that the records are “sought for” an “investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine activities,” the FBI is entitled to the records of anyone at all. Nothing forecloses the FBI from using Section 215 to order a library to turn over all of its circulation records, a business to turn over all of its customer records, or a medical service provider to turn over all of its health records.

Third, Section 215 does not specify any mechanism through which a person served with an order can challenge the order before complying with it. A person served with a conventional subpoena is ordinarily afforded an opportunity to challenge the legality of the subpoena before complying with it. The federal rule governing subpoenas issued in criminal cases, for example, states that the recipient of a subpoena may move the court to “quash or modify the subpoena if compliance would be unreasonable or oppressive,” Fed. R. Crim. P. 17(c)(2). Thus, a medical service provider that received a conventional criminal subpoena for medical records could file a motion to quash the subpoena on the grounds that the subpoena was inconsistent with the Fourth Amendment (which protects “reasonable expectations of privacy,” *see Katz v. United States*, 389 U.S. 347 (1967)), or with statutory law (such as the *Health Insurance Portability and Accountability Act of 1996*, which provides limited privacy protection for health records). A person

served with a Section 215 order, however, is *not* afforded any opportunity to challenge the order before complying with it. The statute does not specify any means through which the recipient of a Section 215 order can lodge constitutional or statutory objections to the order before complying with it.

There is another difference between a Section 215 order and a conventional subpoena that is worth noting. A Section 215 order, like a search warrant, is a judicial command; it is *not*, like a subpoena, merely a request that many ultimately provide the basis for a court order if the recipient refuses to comply and the government decides to seek judicial enforcement. Accordingly, the failure to comply with a Section 215 order would constitute contempt. *See* 18 U.S.C. § 401 (“A court of the United States shall have power to punish by fine or imprisonment, at its discretion, such contempt of its authority, and none other, as...[d]isobedience or resistance to its lawful writ, process, order, rule, decree, or command.”).

Again, there is no doubt that Section 215 could be used to order the disclosure of personal records, including records of personal health information. However, it is impossible to say whether the FBI has used the provision this way already or anticipates doing so in the future. In September 2003, in response to widespread public concern about the scope of Section 215, the Attorney General stated publicly that the FBI had not yet relied on the provision at all, in any context. Unfortunately, it is impossible to verify this statement because Section 215 includes a “gag” subsection that prohibits any person served with a Section 215 order from speaking about the order to anyone else. *See* 50 U.S.C. § 1861(d) (“No person shall disclose to any other person...that the Federal Bureau of Investigation has sought or obtained tangible things under this section.”). Another consequence of the gag provision, of course, is that individuals whose privacy is compromised through Section 215 may never learn of it.

I note, finally, that there is some uncertainty about the future of Section 215. First, a coalition of civil rights, religious, and immigrants’-rights organizations has challenged the constitutionality of the provision. (I am counsel to the plaintiffs in this litigation.) The case is pending in the United States District Court for the Eastern District of Michigan. Second, the Patriot Act includes a “sunset” provision under which Section 215 will expire in December 2005 unless renewed by Congress. It is not clear whether Congress will renew the provision. In his most recent State of the Union address, President Bush urged Congress to renew all of the provisions of the Patriot Act that would otherwise sunset in 2005. *See* President George W. Bush, State of the Union Address, Jan. 20, 2004, available at www.whitehouse.gov (“Key provisions of the Patriot Act are set to expire next year...The terrorist threat will not expire on that schedule...Our law enforcement needs this vital legislation to protect our citizens. You need to renew the Patriot Act.”)

II. Effect of the Patriot Act on government access to information held by subsidiaries of U.S. companies

There is no case law on the specific question whether a United States corporation served with a Section 215 order could be forced to disclose information held by a Canadian affiliate. However, some guidance can be found in cases involving a subpoena served on United States companies with Canadian affiliates.

Representative of these case is *Hunter Douglas Inc. v. Comfortex Corp.*, 1999 WL 14007 (S.D.N.Y. 1999), which involved a subpoena served on United States corporation [*sic*] to comply with the subpoena “to the extent that [it could] exercise custody and control over the relevant documents,” *Id.* at *4. The Court wrote:

In determining whether a corporation within the United States can be compelled to produce documents held by a foreign affiliate, this Court must first consider the nature of the relationship between the corporation and its affiliate....

The test to determine whether a corporation has custody and control over documents located with an overseas affiliate is not limited to whether the corporation has a legal right to those documents....Rather, the test focuses on whether the corporation has “access to the documents” and [the] “ability to obtain the documents.”

Id. at *3; *see also Addamax Corp. v. Open Software Foundation, Inc.*, 148 F.R.D. 462 (D.Mass. 1993) (United States corporation required to comply with subpoena *duces tecum* for documents in custody of German parent); *Cooper Industries v. British Aerospace, Inc.*, 102 F.R.D. 918 (S.D.N.Y. 1984) (United States corporation required to comply with discovery request for documents in custody of British parent).

It is my view that a United States corporation could be forced to disclose information held by a Canadian affiliate, if the United States corporation could access and obtain the documents. That test will likely be met where the United States corporation is the parent. Case law makes clear that the test may also be met where the Canadian corporation is the parent.

Conclusion

The USA Patriot Act seriously compromises the privacy of sensitive records, including records containing personal health information. Section 215 of the Act is of particular concern because (i) it can be invoked against any person, business, or organization in the United States; (ii) it does not include an individualized suspicion requirement; and (iii) those served with Section 215 orders are not afforded any opportunity to challenge the order before complying with it. While a Section 215 order would not be served directly on a Canadian corporation, a Canadian affiliate of a United States corporation could be forced to disclose its records if a Section 215 order were served on the United States corporation. Whether a United States corporation would be required to produce the records of its Canadian affiliate in any particular case would likely turn on the specific legal relationship between the two corporations and on whether the United States corporation could access and obtain the records at issue.