FIPA

BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

Is Government Outsourcing a Threat to Privacy?

A SUBMISSION TO THE INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Examination of USA PATRIOT ACT implications for personal information of British Columbia residents involved in outsourcing of government services to U.S.-linked service providers

August 6, 2004

BC Freedom of Information and Privacy Association
BC Coalition of People with Disabilities

Acknowledgements

FIPA and BCCPD would like to extend our thanks to Will Clements, LLB and the law firm of Fiorillo Glavin Gordon for preparing this submission

We wish to gratefully acknowledge the Law Foundation of British Columbia for their ongoing support of FIPA's activities in the areas of law reform, research and public education

THE LAW FOUNDATION OF BRITISH COLUMBIA

BC Freedom of Information and Privacy Association
103 - 1093 West Broadway, Vancouver, BC V6H 1E2
Ph: 604-739-9788 • Fax: 604-739-9148 • Email: info@fipa.bc.ca • Web: www.fipa.bc.ca

Table of Contents

Executive Summary

The Information and Privacy Commissioner has sought submissions on the potential risks to the security of personal information of British Columbians where administration of that information is contracted out to private sector service providers with links to the United States.

The concern arises in light of the *USA Patriot Act*, which was enacted in the aftermath of the events of September 11, 2001 and gave federal authorities in the United States expanded powers in gathering so-called foreign intelligence information. The crux of the issue is whether the *Patriot Act* could enable the FBI to compel the disclosure of sensitive personal information of British Columbians that has been entrusted by the Provincial Government to a private sector service provider.

The principle that we maintain must be applied to this issue is that the Provincial Government should not outsource any government service where to do so would involve placing sensitive personal information with a private sector entity that could, in *any* circumstance, be confronted with a legal obligation to disclose that information in a manner contrary to the *Freedom of Information and Protection of Privacy Act* ("FOIPPA").

Considering proposed government outsourcing and the potential reach of the *Patriot Act* in light of this principle gives rise to grave concern. Through section 215 of the *Patriot Act*, federal authorities can compel disclosure of documents in the care of a service provider operating in British Columbia whenever the service provider has a branch or affiliate in the United States that is capable of obtaining access. The information need not be limited to persons suspected of a crime. Provided that United States authorities can certify that the information concerns an authorized investigation and the records, which may be "any tangible thing," pertain to foreign intelligence information, an order compelling disclosure will be issued. This amorphous standard can potentially catch a wide range of information pertaining to any number of individuals.

A service provider contracting with the Provincial Government in these circumstances could, in this way, be compelled to disclose the personal information of British Columbians even when disclosure would constitute a breach of the contract that the service provider has entered into, and even when, as we say would be the case, this contravenes the Provincial Government's obligations under FOIPPA.

It follows that our principal conclusion is that the Provincial Government should not outsource any services involving the personal information of British Columbians in any instance where the service provider might, *in any circumstance*, face a conflicting legal obligation to disclose that information to a third party contrary to the disclosure protections in FOIPPA. It is not sufficient to meet the mandatory provisions of FOIPPA for the Provincial Government to be limited to contractual remedies for breach of contract if that were to occur.

Only this approach is consistent with the recognition of privacy as a *right* of all British Columbians. Particularly in the case of sensitive personal information, such as personal medical information, the individual's interest in and right to control of that information is a fundamental human right grounded in our basic notions of dignity and autonomy. The provisions of FOIPPA, and a public body's obligations under it, must be assessed in that light.

I. Introduction

We thank you for this opportunity to offer comment on this significant and pressing issue.

The *USA Patriot Act* came into being shortly following the attacks on the United States of September 11, 2001. The *Patriot Act* was designed to strengthen the national security and information gathering apparatus of the United States, providing in various ways for greater federal authority to collect and share information. It was thus born in a climate of fear and suspicion, a climate that, while understandable, has been seen to give rise to a number of extreme responses that could only be rationalised in light of the horror that was September 11.

The *Patriot Act* has not gone without criticism, and like many other repercussions of September 11, it has implications that extend beyond the borders of the United States. One of these is the subject matter of the present inquiry.

The Information and Privacy Commissioner of British Columbia proposes to examine the impact of the *Patriot Act* on proposed contracting out of public services. Contracting out some public services presents the possibility that access to personal information of British Columbians will be transferred to private sector service providers with links to the United States. The crux of the issue this raises is whether the *Patriot Act* provides a vehicle for federal authorities in the United States to gain access to the personal information of British Columbians that has been contracted out to a private sector service provider, and if so, under what circumstances.

The controversy over this issue was sparked by the proposed contracting out of administrative duties associated with the provincial Medical Services Plan ("MSP") to a company affiliated with a corporation called Maximus Inc. in the United States. The personal information at stake in this arrangement includes the personal medical information of British Columbians who access medical services through MSP, as well as information pertaining to employment and income and whether an individual is criminally incarcerated. In short, highly sensitive personal information.

The starting point for this inquiry, we submit, should be the presumption that the Provincial Government should not entrust the care and control of vital personal information of the residents of British Columbia to any entity that cannot guarantee that it will not face a conflicting legal obligation to share that personal information with others in a manner not contemplated by the *Freedom of Information and Protection of Privacy Act* ("FOIPPA").

Admittedly, potential risks to the security of personal information of British Columbians are many. But this does not alter the fact that FOIPPA does not permit, and British Columbians need not accept, that a proposal by the Provincial Government may contain an inherent, identifiable gap in the Provincial Government's ability to meet FOIPPA's non-disclosure requirements which the public is asked to accept and overlook.

There are, as well, broader issues potentially raised by this inquiry. The concerns presented by the *Patriot Act* are not unique to British Columbia, nor are they unique to the public sector. A cursory examination shows that British Columbians have ample reason to be concerned about the vulnerability of their personal information to unwelcome cross-border sharing when that information is held by private sector companies and other organisations as well. Moreover, concerns are not limited to the *Patriot Act.* Information sharing between the United States and Canada relating to foreign intelligence gathering and criminal investigation is not new; it occurs frequently through a number of existing legal arrangements. And of course, information sharing and disclosure is a potential concern in any foreign jurisdiction, not just the United States.

However, these many broader issues fall outside the issues presently raised and will be left for another day. Although the changes to the *Foreign Intelligence Surveillance Act* ("FISA") achieved by the *Patriot Act* might be described as "small" and "incremental"[1] in the face of pre-existing information sharing mechanisms, they are nevertheless, significant and alarming. The Commissioner's inquiry has raised public awareness and questions about pre-existing methods that authorities in the U.S. use to obtain information about Canadians (the *Mutual Legal Assistance in Criminal Matters Treaty* (MLAT); Grand Jury Subpoenas; National Security Letters, and other law enforcement sharing arrangements). These are also cause for concern, and we would welcome an inquiry into the potential implications of these legal mechanisms on the privacy rights of British Columbians.

Nevertheless, the *Patriot Act* cannot be minimised as nothing more than another small weapon in an already overwhelming arsenal that threatens the security of our personal information.

II. Issues

The Information and Privacy Commissioner for British Columbia has proposed to address the following issues:

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*?

[1] Submission of the Province of British Columbia dated July 23, 2004

III. The *USA PATRIOT Act*

Section 215

While there may be other provisions of the *Patriot Act* that are potentially relevant to this examination, we focus our submissions on the impact of section 215. Section 215 amends the *Foreign Intelligence Surveillance Act* (FISA). FISA formerly provided a mechanism to obtain information concerning a foreign power or agent of a foreign power suspected of being engaged in espionage or terrorism. Now, as summarised below, this power has been greatly expanded by the *Patriot Act,* in terms of both the persons whose information may be sought and the scope of the information that can be demanded.

The key features of Section 215 are as follows:

1. Application for an order to compel disclosure of information is made ex parte to a secret court known as the Foreign Intelligence Surveillance Court (the "secret FISA court"). Very little is known about the process of the secret FISA court. It does not publish decisions when an order is granted.

2. An order from the secret FISA court does not specify its purpose.

3. A person served with an order to disclose information is expressly forbidden from disclosing the existence of the order.

4. Orders apply to "any tangible things;" they are no longer limited to "records" that are in the "possession" of the person served.

5. Any person to whom the territorial jurisdiction of the U.S. courts may extend can be served with an order.

6. There is no individualized suspicion requirement. The information sought may pertain to any person provided the requirements of Section 215 are met. Formerly, it was necessary to specify "specific articulable facts giving reason to believe that the person to whom the records pertained was a foreign power or an agent of a foreign power." No more.

7. Section 215 orders are not limited to criminal investigations. As relates to anyone who is not a United States person, the court shall issue an order if the records concerned are "for an authorized investigation" to obtain "foreign intelligence information." "Foreign intelligence information" includes, among other things, information relating to the national security of the U.S. or the conduct of the foreign affairs of the U.S.[2] It appears, therefore, that if the FBI is able to certify that the information concerns an authorised investigation pertaining to the national security of the U.S., section 215 provides an open door to compel disclosure.

[2] 50 U.S.C. 1801(e)

8. The failure to comply with a section 215 order, or even disclosing the existence of a section 215 order, is punishable as contempt of court.

9. Section 215 provides no mechanism for the recipient of an order to challenge the order. Although the U.S. Department of Justice suggests that recipients may be able to move to quash an order, this has never, as far as anyone knows, been done. Recipients of section 215 orders receive no reasons from the secret court, orders do not specify their purpose, and the rules and procedures of the court are not known. The individuals whose personal information is the subject of the order are unlikely to ever know of the existence of the order, and as far as relates persons in British Columbia who are not U.S. citizens, a challenge that a search is based upon activities protected by the First Amendment of the U.S. Constitution are not available. In fact, if the bare requirements of section 215 are met, it does not appear that the court would have any authority to decline to issue an order, or to quash an order, based upon countervailing interests that are not contemplated by that provision.

10. Owing to the secrecy of section 215 orders, there is no current reliable information as to when Section 215 has been used, for what purpose it has been used, and when it might be used in the future. There is no assurance whatsoever that it will not be used to obtain records held outside the United States, including in Canada, particularly where the investigation concerns "foreign intelligence information" rather than a criminal investigation, making MLAT and grand jury subpoenas inapplicable.

IV. If the Service Provider is an American Company

The terms of reference of this inquiry, quite properly, are broader than simply the proposal concerning MSP. As concerns MSP, we understand that the Government will not be contracting directly with an American company or any company with a business presence in the United States.

Obviously, however, if the Government were to enter a contracting out arrangement with an entity incorporated in the United States or even any company having sufficient presence in the United States to enable a court in the United States to assert personal jurisdiction over it, the *Patriot Act* gives rise to immediate concern.

Any Canadian company with a branch or office in the United States is susceptible to being served with a section 215 order.[3] In that case, the scope of the order would not be limited to information held by the company in the United States, although to the extent that information concerning residents of British Columbia was held in the United States, it would clearly be captured. For documents held outside of the United States, assuming

[3] see *In re Grand Jury Proceedings Bank of Nova Scotia* (1984), 740 F.2d 817

that the approach that would be taken to section 215 orders can be safely analogized to the law relating to document subpoenas, the test is whether the entity served with the order has "control" of the information in question.

The law in the United States concerning what constitutes "control" has been summarized as follows:

> The law is much different in the United States, where SCB Ltd. has chosen to engage in branch banking. Judge Goettel said:
>
> > The law in the United States is that the production of documents may not be resisted merely because the documents are located abroad.
>
> United States v. Chase Manhattan Bank, N.A. and F.D.C. Co. Ltd., 584 F. Supp. 1080, 1085 (S.D.N.Y. Mar. 27, 1984). "The test for production of documents is control, not location." Matter of Marc Rich & Co., A.G., 707 F. 2d 663, 667 (2d Cir. 1983).
>
> The test for "control" is the same whether the documents are required from a party or a non-party. Alcan International Ltd. v. S.A. Day Mfg. Co., Inc., 176 F.R.D. 75, 78 (W.D.N.Y. 1996).
>
> Under Rule 34 and Rule 45, the word "control" does not require that the [*10] party have legal ownership or actual physical possession of the documents at issue; rather documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action." Bank of New York v. Meridien Biao Bank Tanzania, 171 F.R.D. 135, 146 (S.D.N.Y. 1997) (Francis, M.J.).[4]

For information under the "control" of a company that is held outside the United States, such as in British Columbia, compliance with the section 215 order would raise the further questions of whether disclosure under compulsion of a section 215 order would violate British Columbia law, and if so whether that would justify non-compliance. As well, assuming that the terms of any service contract with the Provincial Government would prohibit disclosure, what impact would these contractual obligations have on compliance with the section 215 order?

(i) Violation of B.C. Law?

Whether the obligations of the company regarding information held in British Columbia arise under FOIPPA (as the information is held for a public body) or under the *Personal Information Protection Act,* SBC 2003, c. 63 ("PIPA"), both acts permit the disclosure of personal information without consent, "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 the information (FOIPPA, S. 33(e); PIPA s.18(1)(i)). Any company holding information in British Columbia, and served with a section 215 order in the

[4] *Ssangyong Corp. v. Vida Shoes It'l, Inc,* 2004 Dist. LEXIS 9101

United States in respect of it, would be obliged to ask whether this exception permits disclosure.

The Provincial Government argues that s. 33 (e) of FOIPPA would not permit disclosure for the purpose of complying with an order issued by a court outside of Canada.[5] While we support this conclusion in principle, we are obliged to be more circumspect in interpreting the language of FOIPPA. The language of s. 33(e) is broad and contains no express language to limit the exception to orders issued by courts or bodies within Canada. This is particularly significant when even within the same section of FOIPPA, there is express language that limits other exceptions to, for example, enactments "of British Columbia or Canada" (s. 33(d)). Clearly express language of this kind could have been used in s. 33(e) to limit its scope, had this been the intention of the Legislature.

It is, therefore, at least ambiguous whether s. 33(e) could be successfully invoked to permit disclosure of personal information in compliance with an order issued by a court outside of Canada. The prospect of a section 215 order issued secretly by a secret court for an unknown purpose being capable of providing a legal exception to the protections against disclosure of personal information in FOIPPA, and indeed PIPA as well, illustrate the problem of this ambiguity. S. 33(e) as written potentially provides an unjustifiable and overly broad hole in the privacy protections the legislation was designed to provide. Therefore, we would strongly urge a legislative amendment to clarify (and expressly narrow) the scope of s. 33(e).

For the purpose of this submission, however, we will assume that s. 33(e) does *not* permit disclosure for the purpose of complying with a section 215 order.

(ii) If Compliance Would Violate B.C. Law

Assuming that disclosing information entrusted to a contractor by the Provincial Government would be in violation of FOIPPA, it does not follow that an entity properly served in the United States with a section 215 order could resist disclosure of information held in the province on that basis. Courts in the United States will enforce subpoenas seeking documents held in a foreign jurisdiction even where that places a person in the position of choosing between refusing to comply with the subpoena, and being punished by a finding of contempt of court, or violating the law of the foreign jurisdiction.

In fact, it is open to question whether the secret FISA court would consider, or have any jurisdiction to consider, the competing consideration of conflicting foreign law in, for example, a motion to quash a section 215 order. The issuance of an order is mandatory under section 215 where the requirements of the statute are met, so arguably the provision does not give the court any authority to consider this type of countervailing consideration when an order has been properly requested. Assuming, however, that the secret court would be willing to apply the same "balancing test" that has been used

[5] Submission of the Province of British Columbia dated July 23, 2004

where documents outside the United States have been subpoenaed, the law applied by U.S. courts has been summarized as follows:

> The Second Circuit has adopted a balancing test to determine whether subpoenaed documents maintained by the foreign branch of a United States bank must be disclosed despite local banking secrecy laws. United States v. First National City Bank, 396 F.2d 897, 902 (2d Cir. 1968); cf. Trade Development Bank v. Continental Ins. Co., 469 F. 2d 35, 41 (2d Cir. 1972). In First National City Bank, the Court noted that, "A state having jurisdiction to prescribe or enforce a rule of law is not precluded from exercising its jurisdiction solely because such exercise requires a person to engage in conduct subjecting him to liability under the law of another state having jurisdiction with respect to that conduct." First National City Bank, supra, 396 F.2d at 901 (quoting, Restatement (Second) Foreign Relations Law of the United States § 39(1) (1965)) (emphasis added by Court of Appeals).
>
> The Second Circuit has adopted the approach to enforcement advocated by the Restatement (Second) Foreign Relations Law, supra § 40. Id. 396 F.2d at 902; In re Marc Rich & Co. A.G., 1982 U.S. Dist. LEXIS 10320, M-11-188, slip op. at 17-18 (S.D.N.Y. Aug. 25, 1982); S.E.C. v. Banca della Svizzera Italiana, 92 F.R.D. 111, 115 (S.D.N.Y. 1981); accord, Trade Development Bank, supra, 469 F.2d at 41. Section 40 provides:
>
> > § 30. Limitations on Exercise of Enforcement Jurisdiction.
> >
> > Where two states have jurisdiction to prescribe and enforce rules of law and the rules that may prescribe require inconsistent conduct upon the part of a person, each state is required by international law to consider, in good faith, moderating the exercise of its enforcement jurisdiction, in the light of such factors as [*19].
> >
> > (a) vital national interests of each of the states,
> >
> > (b) the extent and the nature of the hardship that inconsistent enforcement actions would impose upon the person,
> >
> > (c) the extent to which the required conduct is to take place in the territory of the other state,
> >
> > (d) the nationality of the person, and
> >
> > (e) the extent to which enforcement by action of either state can reasonably by expected to achieve compliance with the rule prescribed by that state.
> >
> > The first two factors are of critical importance, the last three appear to be less important, S.E.C. v. Banca della Svizzera Italiana, supra, 92 F.R.D. at 119.[6]

[6] *Ssangyong Corp. v. Vida Shoes It'l, Inc., supra* note 4.

In the case of a section 215 order, when one considers the factors that are considered to be of "critical importance," it is not hard to imagine that the secret FISA court would conclude that an order supporting an authorized investigation that is ostensibly intended to protect the national security of the United States outweighs any hardship that the recipient of an order would face for being obliged to breach FOIPPA.

(iii) Breach of Contract

The FISA court would not hold that a party is permitted to contract out of its obligations under the *Patriot Act*. So, notwithstanding contractual commitments inconsistent with the order, an entity served with a section 215 order can be expected to be compelled to comply with the order. The only issue would then become whether the contractor is liable for breach of contract, and if so what the contractual remedies would be.

As far as the right to privacy is concerned, we submit that this is unacceptable. The right to terminate the contract and claim damages, for example, cannot undo the disclosure of personal information that has already taken place. To contract out the management of information where a section 215 order can potentially compel disclosure, even assuming that such contractual remedies would be available, is inconsistent with the duty to maintain the security of the information in accordance with FOIPPA in the first place.

V. If the Service Provider is a Canadian Company with U.S. Links

A wholly Canadian company that is the subsidiary of a U.S. parent, or that is the parent of a U.S. subsidiary, remains under the potential reach of a section 215 order. The test, as set out above, remains "control." If the affiliated entity in the United States has the ability to obtain the information sought by the order, the information is vulnerable.

In the case, for example, of a service provider that is a British Columbia company, held by a Canadian holding company, which in turn is wholly owned by an American parent company, the chain of ownership makes the records of the service provider in British Columbia potentially accessible by the American parent, and thus vulnerable to a disclosure order. The law in this respect is stated in the submission of Professor Michael Geist and Milana Homsi, quoting *In Re Investigation of World Arrangements*:

> (I)f a corporation has power, either directly or indirectly, through another corporation or series of corporations, to elect a majority of the directors of another corporation, such corporation may be deemed a parent corporation and in control of the corporation whose directors it has the power to elect to office.
>
> (13 F.R.D. 280, 285 (D.D.C. 1952). Qtd. *In re Uranium Antitrust Litigation*, 480 F. Supp. 1138 at 1145.)

This reasoning, admittedly, pertains to "control" of the records of the subsidiary company. The status of records accessible by the service provider through its contract with the Provincial Government, but not *belonging* to the service provider, arguably

differ. In that case, ultimate corporate control might be deemed to be insufficient to give an American parent access to the records for the purpose of a disclosure order. That, however, is a matter of pure speculation. The reasoning could equally be applied to say that ultimate ownership control by an American parent makes records stored by the Canadian service provider accessible notwithstanding that accessing them would constitute a breach of contract and potentially violate British Columbia law.

This reasoning, then, returns the issue to the analysis set out above. If the section 215 order could be enforced against an American parent, to the extent that the contractual and statutory obligations of the Canadian subsidiary might be considered at all, it appears that those issues would fall under the "balancing of interests" approach that considers foremost the "vital national interests of each of the states." As noted above, where the FISA court perceives the order to relate to the national security of the United States, it is not difficult to contemplate a scenario where every possible effort is made to compel an American parent company to access records held by a Canadian affiliate, notwithstanding that it might compel a breach of British Columbia law.

To attempt to insulate a Canadian service provider with an ownership link to an American parent by manipulating the corporate hierarchy and imposing strict contractual terms on the Canadian entity is a legal experiment that risks the vital information of British Columbians.

VI. Requirements of FOIPPA

It appears that a "public body" is permitted to contract out the administration of personal information under its control, and that FOIPPA contemplates the disclosure of personal information to contractors and their employees (FOIPPA s. 33(f), *Vancouver Hospital and Telus,* Investigation Report 01-01).

Nevertheless, the public body must continue to meet the *mandatory* requirements of FOIPPA through its contractual arrangements. In addition, whether or not the custody of personal information is transferred to a third party, the public body must ensure that reasonable security arrangements are made. Section 30 provides as follows:

> 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 disposal.

In approaching these provisions, the public body must indeed have regard for what is "reasonable" and the magnitude of hypothetical risks to the security of personal information. This is not to say, however, that it is acceptable that a system put in place by a public body might in some circumstances be incapable of ensuring compliance with mandatory protections against disclosure of personal information in FOIPPA even when the system is operating according to design. When speaking of what are reasonable security arrangements it is natural to observe that any system of security might be capable

of being breached. An employee might fail to follow an essential protocol, deliberately disclose information, or a computer system might be accessed by a determined hacker. These are inevitable risks, but they are not shortcomings inherent in the security arrangements of the public body that make non-compliance with FOIPPA a specific foreseeable possibility.

The same cannot be said of the risk presented by a section 215 order under the *Patriot Act.* A section 215 order potentially obliges disclosure of personal information by the party contracting with the Provincial Government, or at least presents the potential for a company to be placed in conflict between a U.S. order and its Canadian legal obligations, with uncertain outcome. This risk is thus qualitatively different from these other types of security risks. It is a risk that can be avoided prior to entering contracting out arrangements and is a specifically foreseeable risk inherent to the contracting out arrangement. Contractual remedies, such as providing for termination of the contract and penalties for breach are, to use a colloquial phrase, too little, too late. At that point, vital personal information has been disclosed and FOIPPA obligations abrogated.

VII. Assessing Privacy as a Right

It is significant that this inquiry, while not limited to the proposed contracting out of the administration of MSP, arises in the context of the controversy that proposal has created. The personal information that is thus placed at issue includes personal medical information, which is recognised to touch closely the personal dignity and autonomy of the individual. Perhaps more than in any other area, the right to informational privacy over this class of information emerges as a notion tied to the integrity of the individual that transcends statutory law and crystallizes as a basic human right.

Indeed, the concept of a *right* to privacy must at some point enter the sterile analysis of the requirements of FOIPPA in the face of the *Patriot Act*, and the analysis of what is reasonable action on the part of the Provincial Government when entrusted with the care of particularly sensitive personal information of British Columbians.

People with disabilities, for example, are all too familiar with the stigma attached to many kinds of disability and the discrimination to which access to their medical information can give rise. Barriers to employment, housing, and travel are commonplace. Already people living with HIV/AIDS are barred from entering the United States.

Questions of privacy and confidentiality are not abstractions for people with disabilities; they are concrete daily realities. The possibility, however slight, of their medical records being made available to a foreign agency without their knowledge or consent, and perhaps being further disclosed, is chilling.

A rights-based approach recognises privacy as a social value. This is consistent with a number of international human rights instruments that recognise privacy as a human

right.[7] The *Universal Declaration of Human Rights* at Article 12 provides that no one shall be subjected to arbitrary interference with his privacy. Article 17 of the *International Covenant on Civil and Political Rights* prohibits arbitrary and unlawful interference with an individual's privacy. The *Canadian Charter of Rights and Freedoms*, while not including an express right to privacy, embraces a right to privacy founded on the notion of the dignity and autonomy of the individual. The right to privacy is given specific life through the protection against unreasonable search and seizure in Section 8 of the *Charter* and in Section 7 through the provision that "everyone has the right to life, liberty and security of the person…"

In respect of personal medical information in particular, the Supreme Court of Canada has recognised that when intimate information is disclosed by a patient, it is entrusted for medical purposes and held subject to duties of a fiduciary nature. In *McInerney v. MacDonald,* the Supreme Court of Canada observed:

> The fiduciary duty to provide access to medical records is ultimately grounded in the nature of the patient's interest in his or her records. As discussed earlier, information about oneself revealed to a doctor acting in a professional capacity remains, in a fundamental sense, one's own. The doctor's position is one of trust and confidence. The information conveyed is held in a fashion akin to a trust. While the doctor is the owner of the actual record, the information is to be used by the physician for the benefit of the patient. The confiding of the information to the physician for medical purposes gives rise to an expectation that the patient's interest in and control of the information will continue. [8]

Indeed, we submit that in much the same way British Columbians expect that their personal information disclosed to the Provincial Government under the purview of the Medical Services Plan will continue to be used for their benefit, and that their interest in and control of the information will persist. This concept touches a fundamental human value and imparts fiduciary obligations upon the party in control of the information.

The concept is echoed by the remarks of Madame Justice L'Heureux-Dube in *R v. Osolin*:

> … the interest in the privacy of medical records was recognised in the [*Dyment*] case as a broad and independent value, separate and distinct from considerations about the fairness of the trial process. Thus the privacy interest in *Dyment* may be seen as an interest that pertains to all of us, which may arise in a number of different circumstances. Indeed, it would be odd if the protection of medical records were to be available only to those accused of criminal offences.[9]

Recognising that informational privacy pertaining to personal information, such as medical information, which touches the dignity and autonomy of the individual, is a fundamental value, in fact a human right, necessarily transforms the approach that must

---

[7] BC FIPA, *Personal Health Information and the Right to Privacy in Canada,* Susan Prosser, May 2000
[8] [1992] 2 S.C.R. 138 at 150-51
[9] (1994), 109 D.L.R. (4th) 478 at 490; quoted in *Personal Health Information and the Right to Privacy in Canada, supra* note 7.

be taken to the statutory protections found in FOIPPA when confronted with the *Patriot Act.* When such information is entrusted to the Provincial Government, it is not enough to say that it is "reasonable" for the government to contract out the control of such information because the risk of compelled disclosure to a foreign intelligence service is small and the perceived economic and practical benefits of contracting out are large. Confronting the privacy of British Columbians as a *right*, demands an approach that says the potential abrogation of the right to privacy of British Columbians is unacceptable when the option of not contracting out control of the information is a viable alternative that avoids that risk.

On this point, remarks in a House of Commons Committee Report, *Privacy: Where Do We Draw the Line,* are compelling:

> …. if we approach privacy issues from a human rights perspective, the principles and solutions we arrive at will be rights-affirming, people-based humanitarian ones. On the other hand, if we adopt a market-based or economic approach, the solutions will reflect a different philosophy, one that puts profit margins and efficiency before people and may not first and foremost serve the common good.[10]

VIII. Conclusion

In this submission, we have attempted to focus narrowly, but generally, on the changes to FISA achieved by section 215 of the *Patriot Act* and its implications for British Columbians' personal information involved in the outsourcing of public services to U.S. linked private sector service providers. We have not limited ourselves, nor analysed in detail, the proposed outsourcing of MSP.

In view of section 215, it appears that outsourcing to U.S. linked service providers presents the risk of compelled disclosure of personal information, even when that information is stored in British Columbia, through an order of the secret FISA court. Information relating to British Columbians could be the subject of an order even when no individual whose information is the subject of an order is suspected of a crime, provided that the information is certified by the FBI as sought for an authorised investigation seeking foreign intelligence information. This is an amorphous standard that has the potential to catch a wide range of information pertaining to any number of individuals.

It follows that the Provincial Government's obligations under FOIPPA are potentially compromised. The risk, in our assessment, is unlikely to be eliminated by contractual remedies or conditions placed upon the corporate ownership structure, although it appears that the magnitude of the risk could be mitigated. The principle that we reiterate is that the Provincial Government should not be permitted to contract out a public service where

[10] House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Where do We Draw the Line* (Ottawa: Public Works and Government Services Canada, April 1997) at 33; quoted in *Personal Health Information and the Right to Privacy in Canada, supra* note 7.

to do so has any potential, even if unlikely, to place the service provider in a situation where it is confronted with a foreign legal obligation to disclose personal information contrary to FOIPPA.

Potentially this examination raises wider privacy questions. What about personal information held by private companies? What about pre-existing legal avenues that already provided U.S. law enforcement the ability to compel production of information, even information held outside the United States?

These are important questions that must be asked. And as these issues have been raised in the context of the current request for submissions by the Office of the Information and Privacy Commissioner, we hope that there will be further inquiry to explore those questions. These outstanding questions are not, however, reason to minimise the importance of responding to the specific concern presented by the *Patriot Act.* While seeking to avoid the reach of the *Patriot Act* may be an incremental step in the midst of a web of privacy concerns, it is an important step and we thank the Information and Privacy Commissioner for the opportunity to offer these submissions on the issue.

IX. Recommendations

The examination of this issue should be governed by the following principle:

1. **Government outsourcing should not place sensitive personal information in the care of a service provider that has any potential to face a conflicting legal obligation requiring disclosure of personal information contrary to FOIPPA**

   To the extent that this principle may be compromised, outsourcing of public services should not be permitted. If outsourcing is considered, the following requirements should be assessed as potentially mitigating the risks associated with proposed outsourcing:

2. **Limit outsourcing to contracts with Canadian companies with no business presence in the U.S.**

3. **Seek an international agreement with U.S. authorities concerning the application of Section 215 to the personal information of Canadians stored in Canada**

4. **To the extent of any affiliation of the service provider with an American entity, ensure the U.S. affiliate has no ability to access information held by the Canadian service provider**

5. **Amend FOIPPA to clarify that s. 33(e) does not permit disclosure of personal information for the purpose of complying with an order issued by a court outside of Canada**

6. **Ensure that all data which includes personal information is stored and processed in British Columbia**
7. **Contracts should confirm that information remains in the control of the Government of British Columbia**
8. **Service providers should be contractually obliged to disclose requests for third party disclosure and service upon the service provider of any disclosure orders, from any jurisdiction, to the Provincial Government**
9. **Service providers expressly should not be authorised to comply with any third party disclosure request or order for disclosure from any jurisdiction**
10. **Contracts should include mandatory audit requirements to reveal any unauthorised access or disclosure of personal information**
11. **Contracts should expressly provide a right to terminate the contract upon unauthorised third-party disclosure and specify damages upon breach**
12. **Subcontracting by the service provider should be prohibited**
13. **Recommendations 5. through 12. above should be statutorily mandated through amendments to FOIPPA.**

Submitted by:

Darrell Evans
Executive Director
BC Freedom of Information and Privacy Association

Margaret Birrell
Executive Director
BC Coalition of People with Disabilities