.

SUBMISSION OF

THE BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION TO

THE INFORMATION AND PRIVACY COMMISSIONER

FOR BRITISH COLUMBIA

ON

IMPLICATIONS OF THE USA PATRIOT ACT

ON

GOVERNMENT OUTSOURCING

August 6, 2004

Introduction:

The mandate of the British Columbia Civil Liberties Association (BCCLA) is to preserve and extend civil liberties and human rights in British Columbia and across Canada. We are a charitable, non-profit society.

Privacy is an important part of the BCCLA's mandate. Over the years, we have become a leading advocate for privacy rights of British Columbians and we have been involved in a number of high profile dossiers in this area, including the *Anti-Terrorism Act* and the API-PNR database.

The Privacy Commissioner is conducting an inquiry into the following two 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?

The immediate context for this inquiry is the Province's contracting out of the Medical Services Plan (MSP) and Pharmacare administration to Maximus, an American-based company. Our submission will address this context specifically, and make more general comments where those are warranted.

BCCLA's submission will make the following points:

1. The personal information at issue requires the highest order of privacy protection, not only under the *Freedom of Information and Protection of Privacy Act* ("FOIPPA"), but as engaging constitutionally protected privacy rights.

2. The potential for United States authorities to access databases like MSP and Pharmacare is real and actual. Existing mechanisms for data sharing, such as the Treaty between the Government of Canada and the United States of America on Mutual Legal Assistance in Criminal Matters ("MLAT"), are not analogous to the Patriot Act.

3. The Province's proposal for contractual and corporate structuring means of preventing access to the records do not appear feasible.

4. Where there are credible legal opinions and arguments to both justify and oppose the proposed outsourcing, the Commissioner should employ a Precautionary Approach which would prohibit putting the personal information of British Columbians at risk.

1. The personal information at issue requires the highest order of privacy protection, not only under the Freedom of Information and Protection of Privacy Act ("FOIPPA"), but as engaging constitutionally protected privacy interests.

Section 30 of the FOIPPA provides:

> 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 determining what constitutes a "reasonable security" arrangement under section 30 of FOIPPA, the nature of the privacy interest at issue needs to be assessed.

Citizens have the very highest degree of privacy interest in the kind of personal information that is contained in the Medical Services Plan and Pharmacare databases. As stated by McLachlin J. (as she then was):

> The values protected by privacy rights will be most directly at stake where the confidential information contained in a record concerns aspects of one's individual identity or where the maintenance of confidentiality is crucial to a therapeutic, or other trust-like relationship (*R. v. Mills* [1999] 3. S.C.R. 668 at para. 89).

The American approach to privacy is arguably much weaker than that of Canada or the European Union. In response to European Union Directive 95/44 which makes the transfer of personal data out of the EU country in question conditional upon the existence of "adequate" protection systems, the US instituted a voluntary "safe harbour" system which invited companies to pledge to a series of privacy protection guidelines. The performance of the US under the Safe Harbour Agreement has been severely criticized for failing to attract companies into voluntary compliance with privacy protection standards, failure of voluntary signatories to actually comply with the standards and failure to provide an effective enforcement procedure.

But even prior to the poor performance under the Safe Harbour Agreement, the agreement was criticized for fundamentally misconceiving the nature of the rights at stake:

> The [Trans Atlantic Consumer Dialogue] statement points out that US safe harbour system would not provide European citizens with the adequate levels of protection that they are guaranteed under EU law. Under the EU directive on data protection, privacy is treated as a matter of legal right, with a system of enforcement by public authorities. Under the US safe harbour proposal, privacy is treated more as a matter for negotiation and enforcement is largely a matter of industry self-regulation.1

The BCCLA submits that a similar misconception is at the root of the government's move to outsource the administration of British Columbian's personal health information. There is a critical difference between a legal and ethical culture that sees privacy as an enforceable right and a legal and ethical culture that merely factors privacy into a "business case". There is no doubt that Canadians have a reasonable expectation of privacy of their health records (*R. v. O'Connor* [1995] 4 S.C.R. 411) or that an order to produce such documents is a search and seizure within the meaning of section 8 of the *Charter of Rights and Freedoms*. Therefore, in addition to there being a basic moral justification for protecting privacy as an important part of the autonomy and integrity of human beings, British Columbians have a statutory right to privacy (FOIPPA) *and* a Constitutional right to privacy under sections 7 and 8 of the *Charter*.

Given the critical importance of the privacy interests at stake, the Province acts illegally and unconstitutionally if it unjustifiably violates these privacy rights, or treats such rights as if they were a matter of contractual negotiation.

2. The potential for United States authorities to access databases like MSP and Pharmacare is real and actual. Existing mechanisms for data sharing such as the MLAT are not analogous to the Patriot Act.

Some of the submissions to date have attempted to quantify the risk of the FBI using the Patriot Act to access the MSP and Pharmacare databases by means of that Act's jurisdiction over the US parent company of Maximus.

---

1 "Consumer Group Warns That Safe Harbor Privacy Proposal Will Undermine Consumers' Legal Rights (30 March 2000), online: Trans Atlantic Consumer Dialogue http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/press.cfg&id+2.

The Province and Maximus have both submitted that the risk of US authorities using the Patriot Act in this way is minimal. Both point to the existence of the Treaty between the Government of Canada and the United States of America on Mutual Legal Assistance in Criminal Matters ("MLAT") and other information access mechanisms as more likely to be employed than the Patriot Act. As the Province notes in its submission, MLAT requires that the US authorities first try to obtain records located in Canada through the assistance of Canadian authorities. This "first resort" requirement leads the Province to believe that "in most cases, the U.S. government would seek to obtain records held in Canada through the MLAT before resorting to seeking a Patriot Act order."

The Province concedes in its submission that the MLAT mechanism for exchanging information is restricted to information sought in connection with criminal investigations while the Patriot Act mechanisms extend to obtaining information pertaining to terrorism and intelligence activities. The added risk of access under the broader mandate of the Patriot Act is, in the opinion of the Province, "nominal". The BCCLA submits that the broader mandate of the Patriot Act makes the range of information that can be sought under that mechanism substantially more expansive and greatly increases the risk of access. Further, unlike the MLAT mechanisms, the Patriot Act mechanisms are designed to be secret. Thus, MLAT is largely irrelevant to a discussion of the risks under the Patriot Act.

Prior to the Patriot Act, US authorities had various mechanisms for accessing information sought in connection with criminal investigations. The Patriot Act did not merely incrementally increase the US authorities' available powers of information access. The Commissioner is aware of the expert legal opinion contained in Exhibit "C" appended to an Affidavit filed in the Supreme Court of British Columbia at Victoria, B.C., February 24, 2004 by Mr. Jameel Jaffer, Staff Attorney for the National Legal Department of the American Civil Liberties Union. Some of the key points contained in that document and reiterated in other submissions are outlined briefly below and speak to the extent to which the US authorities' access to information under the Patriot Act has expanded.

While the stated aim of the Patriot Act is to combat terrorism, there is no need for the FBI seeking an access order under section 215 of the Patriot Act to show that the person(s) whose information is sought is an agent of a foreign power or is suspected of any criminal activity whatsoever. There is no required "probable cause". The purpose of the investigation doesn't need to be an investigation into terrorism, but need only "relate" to national defense or security of conduct of foreign affairs. The secret court which authorizes s. 215 orders must grant the order if the application meets the requirements and the Department of Justice does not have to report to either the secret court or to Congress on records actually seized or their usefulness.

Section 215 is *specifically intended* to authorize the FBI to obtain information about people who are not targets of criminal investigations. Simply put, the FBI didn't need the Patriot Act to investigate suspected terrorists; it could always do that. The Patriot Act is a radical expansion of prior powers, greatly enlarging the scope of search and seizure powers that exist under the auspices of criminal investigations. It is *meant* to permit "fishing expeditions" even where one wouldn't expect to find fish.

The US has invested very heavily in an information-based approach to stopping terrorism. The US General Accounting Office report of May 2004 enumerates almost 200 data-mining initiatives of the US government and illustrates the great extent to which the US Departments of Defense and Homeland Security are drawing on an astoundingly broad range of private and public sector databases for data-mining projects. 1[1]

The New York Times recently reported that the US Census Bureau response to a Freedom of Information Act request by the Electronic Privacy Information Center shows that the Bureau has provided specially tabulated population statistics on Arab-Americans to the Department of Homeland Security. The information is detailed to the degree that it provides ZIP-code level breakdowns of Arab-American citizens sorted by country of origin.2[2]

The US is not confining its data compilation efforts to its own country. To cite only one example, the European Parliament has filed an application with the European Court of Justice to quash an agreement struck between the European Commission and the US to provide the US Bureau of Customs and Border Protection with extensive airline passenger information including passengers' meal choices. The challenge to the agreement is that it is in breach of EU privacy laws.3[3]

1[1] Caron Carlson, "GAO Report Reveals Rampant Federal Data Mining" (27 May 2004), online: eWeek.com http://security.eweek.com.

2[2] Lynette Clemetson, "Homeland Security Data on Arab-Americans (30 July 2004), online: The New York Times, http://www.nytimes.com/2004/07/30/politics/30census.html?.

3[3] Simon Taylor, "European Parliament Tries to Quash Passenger Data Deal (30 July 2004), online: IDG News Service Network World, http://www.nwfusion.com/news/2004/073europparli.html.

Is there any reason to believe that the US is not likely to use its expanded powers under the Patriot Act to augment its information-based approach to security? The reason cited by the Province is the US Attorney General's announcement that the Patriot Act's section 215 had not even been used in the first two years of its being enacted. However, FBI internal memos disclosed in an American Civil Liberties Union legal action show that the provision was used just weeks after the US Attorney General's announcement.4[4] Because of the inability to get the appropriate disclosure, it isn't known how many times this provision has been used since the fall of 2003. The US Department of Justice report on the use of the Patriot Act does not include any mention of section 215, but does state that the Department has "moved aggressively" to implement other sections and that one of the purposes of the Patriot Act is to "bring down the wall" that prevented law enforcement and intelligence gathering agencies from sharing information. The report details the great extent to which the Patriot Act provisions have been used in ordinary criminal investigations and how effectively the provisions have expedited surveillance in a myriad of circumstances, only some of which are terrorism related.5[5]

The US Department of Justice claims that the information as to even how often section 215 of the Patriot Act has been used is "classified".6[6] In July 2004, a US legislative effort to prevent s. 215 from being used in order to demand records from libraries was defeated. While members of the American Library Association say that they suspect that the government has been using the Patriot Act to access library records, that is based on anecdotal evidence.7[7] In the face of a refusal to "declassify" even the number of times the provision has been used, the only evidence available is anecdotal. Anyone who has been served with such an order is "gagged" by the provision from disclosing the fact.

The case for quantifying the "risk" of the Patriot Act being used against a database like MSP or Pharmacare will be, by necessity, speculative. But the BCCLA submits that it is clear that the US is demonstrating a voracious appetite for the acquisition of personal data in its efforts to prevent terrorism. The Patriot Act dramatically increases the overlap between US intelligence

---

4[4] "New Records Show That FBI Invoked Controversial Surveillance Powers Weeks After Attorney General Declared that Power Had Never Been Used" (17 June 2004), online: American Civil Liberties Union of Minnesota http://www.aclu-mn.org/17jun20042.html.

5[5] U.S. Department of Justice, "Report from the Field: The USA Patriot Act at Work" (July 2004), online: http://www.lifeandliberty.gov/docs/o71304_report_from_the_field.pdf at 2, 3, 5.

7 Eric Lichtblau, "Effort to Curb Scope of Antiterrorism Law Falls Short" (09 July 2004) The New York Times.

7[7] *Ibid.*

and US law enforcement and does so in ways that are explicitly meant to circumvent the traditional due process protections of state surveillance.

The Province professes itself confident that the US would notify Canadian authorities through the MLAT mechanism if it sought access to databases like MSP because the US would not wish to jeopardize its diplomatic relations with Canada. The entire *point* of the Patriot Act is lost in that analysis. The Patriot Act allows US authorities access to entire databases that they otherwise could not access and further, allows for that access to be obtained entirely in secret. The US does not risk its diplomatic relations with Canada by employing the Patriot Act in this manner. Further, US security priorities do not appear to have been modified by that country's concern with diplomatic relations as can be seen by the US insistence on passenger information from EU countries and the pressure on Canada, the alleged "weak link" in continental security, to conform with US security measures.

Finally, the BCCLA believes that there is little comfort in the possible "sunsetting" of the Patriot Act. While it is at least theoretically possible that portions of the Patriot Act could be "sunsetted" in 2005, it is not considered very likely. Raising the spectre of what 'might be' it must be noted that the Patriot Act has already been expanded with very little notice. Additionally expanded surveillance powers were granted to the FBI, with considerable stealth, under the Intelligence Authorization Act for Fiscal Year 2004 and the US Department of Justice has a number of legislative initiatives that expand surveillance powers even further.8[8]

For example, the proposed Domestic Security Enhancement Act (called "Patriot 2") goes further than the Patriot Act in dismantling court review of surveillance, further expands the reach of an already over-broad definition of terrorism and authorizes arbitrary detentions by rescinding authority for immigrants to challenge the lawfulness of government action by habeas corpus.9[9] The proposed Vital Interdiction of Criminal Terrorist Organizations Act of 2003 ("VICTORY Act") is another new bill that indicates that there is a clear effort on the part of the US government to continue to expand and permanently enshrine the kinds of extraordinary surveillance powers that were instituted by the USA Patriot Act. The VICTORY Act would

---

8[8] David Martin, "With a Whisper, Not a Bang: Bush Signs Parts of Patriot Act II into Law Stealthily" (24 December 2003) The San Antonio Current online: http://www.sacurrent.com/site/news.cfm?newsid=10705756&BRD=2318&PAG+461&dept.

9[9] "ACLU Fact Sheet on PATRIOT Act II" (28 March 2003), American Civil Liberties Union online: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12234&c=206.

increase subpoena powers, provide more leeway over wire-tap evidence and classify some drug offenses as "terrorism".10[10]

In summary, the specific risk that the Patriot Act poses to the privacy of British Columbians' health information cannot be ascertained with accuracy. However, almost every iota of information that has been gleaned about the use of that Act has been fought for. The US Department of Justice is successfully keeping almost all information about the use of the most controversial provisions of the Patriot Act classified. But a dearth of direct evidence does not prevent us from making fair suppositions. We submit that, for all the reasons above, the Patriot Act is a real risk to the privacy of personal information contained in databases that could be accessed through American-linked companies.

3. The Province's proposal for contractual and corporate structuring means of preventing access to the records do not appear feasible

The Province has submitted an outline of a proposal to prevent or limit access to records through contractual and corporate structuring means. The Province says that it is "currently considering" a structure that we understand as follows: a US subsidiary (Maximus CAN) holds a beneficial interest in the shares of Maximus Service Provider which has direct custody and control of the records. The shares in Maximus Service Provider are owned by an independent trust company and the trustees are obliged to transfer ownership of the shares to the BC government in the event that the US government directs the parent corporation to turn over the records of Maximus Service Provider.

If we have understood this proposal correctly, it allows for the expropriation of assets in the event that access to the records is threatened and thereby ensures that the records in question cannot be subject to the Patriot Act. If the proposal is as we outline above, we think the safeguarding of the records by the proposed means is quite strong. However, we also think that it is not very likely that Maximus, or any other company for that matter, is going to agree to an expropriation of its assets on the basis of a triggering event over which it has no control. In other words, this structuring seems appropriate to the protection of the records, but doesn't appear to be feasible in practical terms.

10[10] Dean Schabner, "Draft Bill Would Provide Broader Power; Ashcroft Defends Patriot Act" (20 July 2003) ABC News online: http://abcnews.go.com/sections/us/WorldNewsTonight/victory_act030820.html.

It is important to note that the Province has outlined a number of privacy protection measures that it says "will be deployed on a case by case basis" to outsourcing initiatives and some legislative amendments to the FOIPPA. The mitigation strategies that are directly aimed at dealing with the risks of the Patriot Act are under consideration and currently consist of point-form outlines. The proposals themselves are tentative, and clearly the actual drafting of the instruments will be a critical aspect of ensuring that the proposed protections meet the objectives. The Province states that which mitigation strategies should be implemented in a given case depends on how sensitive the records in question are. Without question, the MSP and Pharmacare databases require the most stringent mitigation strategies. Theoretically, this is possible through elaborate corporate structuring and expropriation contingencies, but the Province has made no guarantee that it will do so. The Province has outlined a series of measures that it is "considering". For all that the Province's submission is very lengthy, it nevertheless fails to state what the Province is committed to doing as opposed to what it *might* do.

It should be assumed that the Province understands that the kinds of expropriation measures mentioned in its proposal are beyond extraordinary. We submit that these extraordinary measures do appear to address the threat of the Patriot Act, at the same time that we submit that there is every reason to believe that such measures will be considerably watered down in contract negotiations.

4. Where there are credible legal opinions and arguments to both justify and oppose the proposed outsourcing, the Commissioner should employ a Precautionary Approach which would prohibit putting the personal information of British Columbians at risk.

A public body that needlessly exposes personal information in its custody and control to risks of unauthorized access is in breach of FOIPPA. It is the BCCLA's position that only a security arrangement which effectively eliminates a risk of unauthorized access can be found "reasonable" where the risk is undertaken voluntarily. Put another way, no security arrangements are "reasonable" which seek merely to partially mitigate a serious risk that is undertaken voluntarily.

The BCCLA has no position on outsourcing generally. However, where the outsourcing involves risks to privacy, the Association does take issue. In the instant matter, there is risk of unauthorized access to highly sensitive personal information . Because there is no need to outsource to a foreign company, the risk is being assumed voluntarily. The policy laundering

argument that NAFTA-Made-Us-Do-It does not have any application to the facts; the government has a choice as to how it will deliver these services. The decision to outsource was undertaken voluntarily and the purported (not proven) benefits are said by the government to be increased efficiency. There is no case law that is directly on point in regard to how serious the risk of authorized access through the Patriot Act could be. There are vastly differing opinions on the gravity of the risk, as well as on the benefits that are claimed to flow from assuming the risk.

In these circumstances, we urge the Privacy Commissioner to take a Precautionary Approach. Previous Privacy Commissioner, David Flaherty, stated that "privacy protection is about balancing competing interests". In the instant matter there is unknown but real risk of unauthorized access to personal information and an unknown but purported benefit to contracting out to a US-linked company. The only thing that is not in dispute is the level of privacy interest at stake. The privacy rights at issue are the most fundamental. There is no more sensitive informational data than personal health records. In this circumstance, the "reasonable" security measure is one of caution.

The Province has clearly stated (para. 3.19) that it does not believe that a breach of section 30 of the FOIPPA warrants an order that the public body can no longer disclose personal information to a contractor. The Province submits that a finding of a section 30 breach only warrants an order requiring the public body to implement such security measures as are appropriate in the circumstances.

We submit that the question of what is an appropriate security measure in the circumstances is riddled with unknowns and that, given that the Province is proposing to essentially make an experiment of British Columbians' personal health information, the Privacy Commissioner *is* warranted in making an order that the public body not disclose personal information to the contractor. We submit that the authority for such an order is found in FOIPPA in sections 42 and 58:

General powers of commissioner

42(1) In addition to the commissioner's power and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may

(a) conduct investigations and audits to ensure compliance with any provision of this Act,

(b) make an order described in section 58(3) whether or not a review is requested

Commissioner's orders

58(3) If the inquiry is into any other matter, the commissioner may, by order, do one or more of the following:

(e) require a public body to stop collecting, using or disclosing personal information in contravention of this Act, or confirm a decision of a public body to collect, use or disclose personal information

In conclusion, we believe that the precautionary principle is appropriate in this case and we urge the Commissioner to assess the matter in that light.

All of which is respectfully submitted.

Micheal Vonn

Policy Director

British Columbia Civil Liberties Association