

Public-sector Outsourcing and Risks to Privacy



Office of the Information and Privacy Commissioner

Alberta

February 2006

Introduction

This report focuses on public bodies — provincial and local — under Alberta’s *Freedom of Information and Protection of Privacy Act* (“FOIP”). These bodies maintain population-wide information systems carrying sensitive personal information. Participation in many of these information systems is not a matter of choice for Alberta citizens, who naturally remain vigilant over how their personal information is protected by public bodies. The Legislative Assembly of Alberta has addressed issues of access and privacy for Albertans’ government records through the FOIP Act, enacted in 1994 and updated in 1999 and again in 2003. The FOIP Act sets up the Office of the Information and Privacy Commissioner to oversee how public bodies collect, use, disclose and look after the personal information of Albertans.

This report looks at public-sector outsourcing in Alberta with an eye to the risks it presents and to how these risks can be mitigated. The issues raised here can have implications for private-sector information management, and for health-services work beyond the range of our regional health authorities. However, the scope of this report is limited to just the outsource practices of “public bodies” as defined in the FOIP Act, including provincial ministries, boards, agencies and commissions, as well as local bodies such as school districts, public post-secondary institutions, hospitals, and municipal governments.

Outsourcing of information and communications technology (“ICT”) functions by public bodies has become a high-profile issue in terms of privacy and security since the topic was raised in a 2004 British Columbia court case. That challenge by a public-service union against a government outsourcing plan prompted the Information and Privacy Commissioner of British Columbia to issue a report in October 2004 titled *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*. Following publication of that report, the Office of the Information and Privacy Commissioner of Alberta felt that it would be important to look at the extent of this kind of outsourcing in Alberta to understand what was being outsourced, what risks this presented, and how those risks might be dealt with.

We believe that foreign laws such as the UPA were only one of the many challenges presented by outsourcing and that the UPA issue had been ably canvassed in British Columbia. Together with the Government Services Ministry of the Alberta Government, we developed a survey to send to all provincial government ministries and to a representative sample of local public bodies. The survey canvassed the extent of outsourcing by public bodies, the kinds of functions outsourced, and the contractual basis of the outsourcing. The Office of the Information and Privacy Commissioner analyzed survey results to assess the current state of public-sector outsourcing in Alberta, with a view to producing recommendations appropriate for Alberta.

Table of Contents

1. Alberta's Outsourcing Experience

- 1.1 Overview of Outsourcing in Alberta
- 1.2 The basic outsource business model
- 1.3 Location of large-scale operations
- 1.4 Alberta's early entry into outsourcing
- 1.5 Outsourcing and the FOIP Act
- 1.6 Alberta Government policies on outsourcing

2. Outsourcing and Privacy

- 2.1 Introduction
- 2.2 The risks from public sector outsourcing
- 2.3 The USA PATRIOT Act – a Particular Concern?
- 2.4 Personal information and the “war on terrorism”

3. Current-state Review of Outsourcing Agreements

- 3.1 Alberta's 2005 Outsource Agreements Survey
- 3.2 Results from Alberta Government ministries
- 3.3 Results from municipal government and police services sector
- 3.4 Results from the public post-secondary institution sector
- 3.5 Results from the K-12 schools sector
- 3.6 Results from the health-care sector
- 3.7 General observations from the 2005 Survey

4. Strategies to Mitigate Risk and Improve Privacy

- 4.1 The range of measures to consider
- 4.2 OIPC recommendations for Alberta Government action
- 4.3 Commissioner's conclusions

Appendix A: Literature Review on Outsourcing

1. Alberta's Outsourcing Experience

1.1 Overview of outsourcing in Alberta

In the 1980s a number of converging developments in technology and public management theory led to new thinking about how government work can most efficiently be done. The combination of flexible, portable database tools and new digital electronic communications capabilities opened up the possibility of doing government work in different, possibly more efficient ways, sometimes outside of usual government premises and business hours, by outside parties expert in applying business solutions to administrative challenges.

By the early 1990s, certain public bodies in Alberta were adopting strategies to outsource their administrative functions. Systems consolidated during the 1980s (e.g., motor vehicles, student loans, health care insurance, payroll administration, etc.) became the subjects of calls for proposals to companies which could take them over and manage them on behalf of the public bodies. (These companies sometimes call themselves “solutions suppliers” or “business process operators”; we will call them “outsource providers” in this report.) In some cases, the marketplace provided an array of outsource providers available to take on the task. In other cases, particularly where a complex, interactive set of functions was to be outsourced (e.g., employee payroll/pension administration), public bodies initiated a process to actually establish an outsource provider and get it up and running as a government-sponsored enterprise. Sometimes these more complex outsourcers were joint ventures combining a technology expert with a business process expert. And in some of these joint ventures the public body itself would be a participant or stand as part-owner.

The public bodies embarking on outsource projects focused on cost-effectiveness. The concept of achieving savings was ever present, though projects would, in many cases, involve higher levels of investment in their early stages. Public bodies looked heavily to the outsource providers to find ways of delivering a return on investment by exploring structural and technological options for getting the work done more economically.

Outsourcing became a strategy for a wide range of government programs. By 2005, the largest outsource application (measured as expenditure) for the Alberta Government was not in any information technology field but rather in the maintenance of its highways. But outsourcing information and communications technology systems figured highly in the movement to outsource, and recognizable ‘tier-one’ ICT companies currently occupy second and third place in the dollar ranking of service vendors to the Alberta

Government. This report considers only ICT-related outsourcing, including as well any outsourced arrangements for records storage.

1.2 The basic outsource business model

The business model for outsourcing was that outsource providers would find savings for their clients, and make their own profit margins, through increased efficiency. That efficiency would be found by concentrating computer operations, by using proprietary software and by building management and technical staff groups outside the civil service capable of applying proven solutions for different clients having common business problems.

Another place to find efficiencies was in the expensive area of communications facilities. Here the spread of the World Wide Web and the digital communications revolution opened up the possibility of instantaneous movement of data to any part of the world and the prospect of moving work into countries with less-costly factors of production.

Outsourcing was perceived as a chance to solve a number of problems for public-sector organizations.

- Cap the drain of investment resources going towards unending ICT systems projects, thereby allowing public bodies to direct resources back to core client-service functions.
- Reduce the inconsistencies and incompatibilities among government systems, allowing the integration of common programs and services.
- Address the inefficient utilization of data-storage facilities, a major ICT cost component.
- Lead to the adoption (or importing) of innovative service models that would improve customer access, convenience and satisfaction.
- Facilitate access to leading edge technology.
- Share the risks of program delivery with private sector partners.
- Capture the experience and creativity of private sector partners.

1.3 Location of large-scale operations

The larger potential outsource providers, many already established as trans-national corporations headquartered outside Canada, hold distinct advantages in operating on global channels. For some large-scale outsource projects, these major corporations would be the only available organizations capable of assuring service delivery to the standards required by the public bodies. That factor, and the lack of private-sector data-centre capacity in Alberta would mean that large systems would be outsourced to major companies operating ‘in-house’ on the Government of Alberta’s own computer installations, or to those

same companies using databases housed outside Alberta or occasionally moved outside Alberta for development testing and maintenance work. (Note: Over the past decade, there has been a significant change to this situation, with the development of considerable data centre capacity in Alberta, centred predominantly in Calgary).

1.4 Alberta's early entry into outsourcing

Public bodies in Alberta had outsourced significant portions of their administrative functions ahead of the arrival of access and privacy laws. (Outsourcing and its companion, downsizing, were both means and ends of the "New Public Management" movement that surged across fiscally-troubled governments in the early 1990s. These developments are described in materials covered by the literature review appended to this report).

Alberta's FOIP Act came into effect in late 1995, and did not govern the full local-public-body realm until late 1999. Yet, while some other Canadian jurisdictions would not adopt alternative service delivery approaches until recently, the Government of Alberta moved a full decade ago (along with New Zealand, Australia and the United Kingdom) to outsource certain database programs. The use of outsource providers had become commonplace on the Alberta landscape by the mid-1990s, pre-dating the enactment of access and privacy legislation.

1.5 Outsourcing and the FOIP Act

In general terms, these pre-FOIP outsource agreements did align well with the strict requirements of the new FOIP Act, where ultimate accountability of public bodies for the conduct of their contracted outsourcers is a clear principle. Nevertheless there was concern about placing public records in the custody of private operators. This concern was among the factors prompting the 1997-98 joint audit by the Office of the Information and Privacy Commissioner ("OIPC") and the Office of the Auditor General on the Alberta Registries program. In that project, the auditors examined private-sector outsource providers operating as licensed Registries Agents. These invariably were local companies working under a model contract. The access to personal information by external entities was reviewed by the audit team in the context of Registries' sales of driver/owner data to private clients, more a vendor-client transaction than an outsourcing scenario. The major outsource agreement for the management of motor-vehicle-related data, the MOVES system which had been outsourced to EDS Canada, was examined from a security perspective and found to be a safeguarded arrangement.

Another key development in the early years of the FOIP Act was the Alberta Information and Privacy Commissioner's proactive advocacy, and the Government's support, for the 'privacy impact assessment' process to test new information management schemes against the requirements in the Act. Alberta was among the first jurisdictions anywhere to make the drafting and publication of privacy impact assessments a matter of government policy for provincial public bodies. In 1999 they became mandatory for health care custodians under the new *Health Information Act*.

What was becoming clear through events like the Registries audit and the development of the privacy impact assessment process was that the FOIP Act was a major factor in the measurement of acceptability of data management schemes.

1.6 Alberta Government policies on outsourcing

The FOIP Act did prompt policy development work within the Alberta Government to provide guidance on how obligations in FOIP are to be reflected in contract management. In 1997 a *Contract Manager's Guide* was published to address emerging issues in alternative service delivery. It dealt with the outsourcing of program delivery as well as privatization of government functions. The Guide was updated in 1999, becoming both firm direction to Government ministries (and their boards, agencies and commissions) and a model for use by local public bodies. An expanded version, now titled *Guide to Managing Contracts under the FOIP Act*, was released in September 2005 by Alberta Government Services, the ministry responsible for implementation and administration of the FOIP Act.

While the *Guide to Managing Contracts under the FOIP Act* has evolved as the Alberta Government's central access-and-privacy policy on managing information in all manner of contracts and agreements dealing with alternative service delivery, a complementary policy addressing the outsourcing of information and communications technology applications has been issued by the Government's Chief Corporate Information Officer ("CCIO"). That policy has at its source concern over security and privacy expressed by the Information and Privacy Commissioner to the CCIO and other officials in 1998. The concern at that time was not "national security" related factors like the UPA, but the potential for civil or state action being taken against an outsource provider in another country, resulting in the seizure of data facilities and databases. The CCIO suggested public bodies could reduce that risk to security and privacy by limiting outsourcing to within Canada, where the Government could have a reasonable chance of retrieving information under bankruptcy and creditor's rights laws.

The Government's response to the Commissioner having raised the matter of data outsourcing agreements in 1998 was to review existing agreements to determine risk levels from a location-of-asset perspective. The ensuing scan found that the majority of Alberta Government outsource agreements had information held within the Province of Alberta, though a few public bodies stored or processed data containing personal information outside Alberta. The Commissioner encouraged the Government to locate outsourced data processing in Alberta as a first preference, with allowances for back-up storage elsewhere in Canada if necessary. Subsequent guidance from the CCIO to the CIO Council and to deputy ministers was to consider the benefits of locating outsourced data within Alberta or Canada. This recommendation on data location was not expressed as formal policy, but rather was left as corporate advice from the CCIO to the Government's ICT community.

2. Outsourcing and Privacy

2.1 Introduction

The present "outsourcing" issue arose from events in British Columbia in 2004 whereby the Government of British Columbia had planned to retain a US linked contractor to run the province's public health insurance program. The British Columbia Government and Service Employee's Union raised the issue that contractors who possess personal information could be secretly compelled under the UPA to turn it over to US authorities. British Columbia Information and Privacy Commissioner David Loukidelis conducted a thorough review of that issue and wrote a report "Privacy and the UPA" in October 2004.

It is not necessary to duplicate that effort. Our concern here is to broadly outline issues and risks arising from the outsourcing of government programs generally, including risks posed by legislation such as the UPA.

2.2 The risks from public-sector outsourcing

The public body's contract with the outsource provider becomes the primary vehicle through which information risks are managed. In an outsource agreement, the public body defines control over information, but the outsource provider implements control over information. A proper contract sets boundaries and expectations for the outsource provider in terms of its allowable actions in the collection, use and disclosure of personal information.

There exist some direct risks to access and privacy from outsourcing that warrant more detailed analysis and attention in contract formulation. These sources of risk include:

1. Failure to include appropriate controls in the contract.
2. Failure to clarify information ownership, especially where the provider enhances or adds value.
3. Failure to guarantee thorough investigation of information risk management incidents.
4. Failure to guarantee timely reporting of information risk management incidents.
5. Failure to comply with corporate governance, regulatory or legal obligations in relation to the public body's information.
6. Failure to remain solvent.
7. Failure to avoid catastrophic disruption.
8. Failure to assure due diligence, and acquire public body permission, prior to engaging sub-contractors.

Outsourcing brings a series of new risks to information. The following are some of the risks that governments and businesses need to take into account:

- The prospect of losses of data-laden hardware. Many outsource arrangements involve some form of freight handling, with tapes, cassettes, microfiches, *etc.* occasionally vanishing from the chain of custody, normally at points of transfer along the way.
- Data outsourced to offshore operators in other countries has been accessed by outsourcer staff to bilk customers' accounts. (This risk is occurring with increased frequency in high attrition call-centre settings, where employees can gain full particulars about a customer very quickly from outsourced data systems and from direct phone contact with the customer during outsourced business process transactions such as bank transfers and travel reservations).
- We have also observed that the potential for civil property seizure of data facilities operating under foreign jurisdiction can become a concern where sub-contracting is done to a marginally-viable company without doing a due-diligence investigation of that sub-contractor.
- There is the increased exposure to interception of communications and to database hacking from unintended users, ranging from foreign law enforcement authorities to predatory hackers.
- There is the risk that when information is housed outside of Canada it becomes susceptible to the laws of that jurisdiction, such as the PATRIOT Act.
- Property thieves who include data-laden hardware (e.g., laptops, terminals, servers) in their haul.
- Incidental finders of errant or misplaced information, particularly where sub-contracting is involved (though here the risk can range, depending on the moral choices made by the finder).
- States and corporations acquiring the data through civil action seizures of outsourcer assets.

- Foreign law enforcement investigators, particularly those responsible for national security intelligence.

Not all these risks are generated solely by entering an outsource arrangement. Certain risks (computer hackers, rogue employees, property thieves and incidental finders) can be present in some measure even where ICT systems are kept in-house by public bodies. However, outsourcing can expand the opportunities for these problems to occur, thereby enhancing the overall risk. Outsource companies themselves occasionally use sub-contractors and enter their own outsource agreements, sometimes even becoming “customer providers” to larger outsource operations. The chain of users becomes only as strong as its weakest link.

However, the risk of civil seizures and foreign investigators is directly tied up with outsourcing. The last of these unintended users, foreign law enforcement investigators, warrants detailed exploration as it presents a new dilemma for privacy protection.

Discussions of the economic value of outsourcing are not an issue for an Information and Privacy Commissioner. However, from the viewpoint of privacy protection and optimal information management practices, it is important to stay mindful that a decision to handle information internally (i.e., to not outsource) carries its own set of potential risks to privacy. Many government bodies no longer have the capability of doing it right without professional help. Their own development expertise and production know-how has migrated to the outsource services industry, which in Canada now claims 500,000+ jobs earning \$13 Billion in annual revenues (according to the Information Technology Association of Canada, July 2005). The need for continuous testing and the level of fortification of systems environments now required for secure electronic communications and storage is beyond the reasonable capacity of many public bodies. A decision to keep a function in-house may mean denying to the program records a degree of security only obtainable in state-of-the-art outsourcer ICT environments. The critical point is that choosing to outsource in itself does not bring more risk or less risk, but it does entail different risks. It is important to underline that outsourcing does not eliminate risks to data. Indeed, 2005 was a banner year for losses, hacks and spills of personal information in the private sector.¹ While the private sector is getting better at security (they have to), they could learn about privacy from much of the public sector. Both parties could benefit from this synergy.

¹ See for example <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

2.3 The USA PATRIOT Act – A Particular Concern?

The legislative response by the American administration and Congress to the attack on the World Trade Center (“9/11”) was packaged in a series of legal amendments called the USA PATRIOT Act (“UPA”). That law, passed expeditiously as a set of temporary war measures, gave the FBI an expanded national security role and armed it with extraordinary legal processes to acquire personal information (about Americans and about foreign nationals) held by American companies and by foreign companies affiliated with American companies, no matter where those companies were located or whom they were working for. It is important to keep in mind that it is not just the UPA which is of concern in this regard. Many countries likely have UPA-like legislation. Therefore, simply not outsourcing to American or American-linked companies is not necessarily a solution.

The difficulty in the UPA (for purposes of this particular analysis) is that it sets out two control paradigms and one overriding condition:

1. **The Extraterritorial Extension Paradigm:** The UPA uses the concept of corporate links to determine the reach of its long-arm provisions. These links are viewed in terms of ownership or operational relationships. A Canadian company owned by a United States person (e.g., a parent corporation) becomes a US-linked company. A Canadian company with an American subsidiary, or operating in the USA, becomes a US-linked company.
2. **The Tangible Record Paradigm:** The UPA identifies its information objects by the presence of tangible record material. Where tangible material resides beyond American borders with a company affiliated to an American company (i.e., in the custody of a US-linked company), the UPA asserts American jurisdiction to have the extra-territorial company provide the tangible material to American national security police. The UPA targets the keeper of the tangible record, making custody of records its targeting criterion. In outsource arrangements it is the contracted company that normally has that custody.
3. **The Overriding Condition:** The UPA lays a secrecy cloak over the whole process of demand and response, including the secret application of very serious penalties. The UPA’s secrecy requirement makes it difficult to monitor the use of its powers. There is no opportunity for safe whistle-blowing and there is no ability for challenge in open law courts.

Since the PATRIOT Act issue became so highly publicized in Canada in 2004, outsourcers have worked at finding strategies to mitigate the risks posed by the UPA. Outsourcers are exploring how technology strategies using encryption keys held exclusively in Canada can provide access control. Related strategies such as data minimization, anonymization or pseudonymization are also receiving attention from outsource providers and from academic researchers. The hope is that a comprehensive approach combining these types of technology strategies with tighter governance provisions in contracts will provide an effective firewall to protect personal information of Canadians where that information moves across international boundaries. However, as a major Canadian subsidiary of a US-based international outsourcer advises in its paper on *Strategies to Address Privacy Issues under the U.S.A. Patriot Act in Outsourcing*², the only measure that can be considered “an effective, overall response” to the risks of the UPA for companies managing data on a transnational basis is “migrating the data back to Canada.”

Ultimately the net effect of the UPA may be that it leaves location of the data as the lone available control for a government in Canada -- federal or provincial -- to reduce the intrusive impact of the UPA on privacy of Canadians. The easy answer, suggested in some quarters, of protecting privacy by assuring no company affiliated in any way with an American company, or doing business in the USA, is allowed to do outsource work for Canadian governments, fails to recognize the existing transnational nature of the IT services industry. It is difficult to find companies which are not linked to American affiliates. It may be inefficient to set up unlinked companies that could commit to staying unlinked.

Some observers do see room to maneuver by controlling the physical location of information records. This tactic may be effective where a static medium such as paper or microfiche or hard computer disk is involved (e.g., a storage contract for paper files). However, where the movement of digitized information in cyberspace is the lifeblood of an outsourced application, the protective qualities of geographic location may amount to very little.

To the extent that location can have meaning, and that an outsource company can avoid locating tangible information records inside the direct territorial pull of the UPA (forgetting for the moment its controversial extra-territorial claims), one strategy would be to assume that Canadian outsource providers will govern themselves by Canadian law and the provisions of their contracts. When outsource providers are Canadian companies directed by Canadian boards and staffed by Canadian employees, a trust-based solution (where outsource providers monitor themselves) is a consideration. However, the UPA’s overwhelming condition of secrecy makes it unreasonable to rely on trust to assure privacy protection from American national security authorities. Threats

² Constantine Karbaliotis, LL.B., CIPP, *Strategies to Address Privacy Issues under the U.S.A. Patriot Act in Outsourcing*, CGI/GTA Security and Privacy Practice, February 4, 2005.

of harsh consequences for their corporations and prospects of personal career setbacks in transnational career structures combine to make it quite conceivable that outsource company directors or employees might disregard privacy provisions in contracts or even in governing Canadian statutes when a US-court-sanctioned secret demand is made. This makes it impossible for Canadians to address the exposure threat by simply leaving outsource providers to behave on an honour-system basis.

The Information Technology Association of Canada (“ITAC”), with hundreds of corporate members, has emerged as an important voice of the outsource industry on issues of access-and-privacy law. Its recommendations to governments distill the views provided by individual corporations to B.C. Commissioner Loukidelis in his 2004 public consultation on the UPA.

In its July 2005 position paper entitled *The USA Patriot Act and the Privacy of Canadians: Perspectives of the Information and Communications Technology Industry on Delivery Services to the Public Sector*, ITAC argues that the UPA risk is so minimal that it can be disregarded in practice. The industry sees national security policing as routine law enforcement activity where investigators seek information about identified persons. It suggests the UPA powers will not be used as the FBI will call the RCMP when it needs information, and would not take the trouble to secure and scour databases from Canadian outsourcers.

This presumes that law enforcement agents from other countries would use the more effective and customary channels to Canadian law enforcement counterparts to assist in finding information about a named individual’s status or activities in Canada. The depiction here is that national security police work is much like old-fashioned criminal pursuit work, where police use data resources to help them find or watch over an already known suspect.

This position seems to ignore the post 9/11 interest in data fusion (where the goal is to fuse unrelated databases into a resource capable of identifying threatening patterns and of supporting data-mining to find a person or grouping whose activities conform to those patterns). No doubt the pursuing of targeted suspects would follow the treaty-based communications channels through Canadian police as we all expect. But it is not reasonable to expect that a foreign security police service would resort to those channels for clandestine access to population databases for the purposes of milling vast amounts of data. The UPA, which can be invoked against any person, business or organization (including libraries, bookstores, hospitals, ISPs and political parties) does not include an individualized suspicion requirement. It can arguably be used for broad data-netting operations.

Our assessment of the UPA issue takes up from the analysis developed by the Information and Privacy Commissioner for British Columbia in his October

2004 report *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*. In preparing that report, Mr. Loukidelis asked two questions:

1. Does the USA Patriot Act permit US authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of US-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 FOIPPA? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with FOIPPA?

These questions dealt with legal rules very similar to those present in Alberta's FOIP Act (1994), which is based largely on the B.C. (1992) and Ontario (1988) statutes. The BC Commissioner found that the UPA would apply to records physically located in the US. More importantly for our analysis, he commented conclusively on the dilemma facing US-linked Canadian outsourcers:

Further, we have concluded that it is a reasonable possibility that the US Foreign Intelligence Surveillance Court (FIS Court) would issue a FISA order requiring a US-located corporation to produce records held in Canada by its Canadian subsidiary or, indeed, require a person or corporation within the jurisdiction of that court to disclose records held outside the US that they control because they have the legal or practical ability to obtain the records. It has also been said by some US courts that a US-located corporation will control a foreign corporation if the US corporation can, directly or indirectly, elect a majority of the directors of the foreign corporation." (p.132)

The B.C. Commissioner recommended an array of actions, including express blocking provisions, to prevent a Canadian-based outsourcer from disclosing B.C. Government personal information records to the FBI under the UPA.

Even before he had finalized those recommendations, the B.C. Government introduced Bill 73 to bring into force restrictions on how (in future) outsourcers work with public bodies. The B.C. Government then quickly followed through on its stated plan to outsource healthcare information to a Washington D.C. outsource corporation, requiring that company to set up a BC-based subsidiary overseen by Canadian directors and committed to maintaining the medical records inside British Columbia. Around the same time, it outsourced non-tax revenue operations to a Canadian subsidiary of a major US-based international outsource provider, adhering to the same restrictive formulas, including the setting up of a special purpose B.C.-based subsidiary to manage the outsource

agreement and safeguard the data inside British Columbia. Since these restrictions were enacted, there has been controversy over their effectiveness.

2.4 Personal information and the war on terrorism.

For all the attention it attracted, it is likely that the UPA only represents one means of gathering information for national security purposes. It is not clear whether the PATRIOT Act, section 215 in particular, is limited to investigations of specific individuals or if it can be used to obtain entire databases. In his report, at pages 69 to 71, Commissioner Loukidelis says at page 71:

Critics say that the expansion of the power to make FISA orders to any tangible things”, combined with no limit on the number of records obtained, means FISA orders may not be made in relation to entire databases of information.

Of course, since FISA orders are secret, it is difficult or impossible to say if one has ever been used to obtain an entire database. Even if it has, it is not clear that gathering and “fusing” a number of disparate databases would yield much useful intelligence. To quote Joel Brenner, former Inspector General of the United States National Security Agency:

Gathering all the bits of data floating around in the hope that you can sort through it all – in effect, swallowing the sea – is a fatuous idea. No organization, and no technology, can do it.

The challenge now is aligning the technologies and database architecture of the many military and civilian organizations and agencies that produce or consume sensitive information at the federal, state and local levels. Doing this right will require more time and more money, lots of it; and the task will never be finished because the technology is changing constantly.³

It is likely that, in the aftermath of the events of 9/11, there will be more collection of more information and more disclosure of this information to more individuals and agencies.

The issue of information sharing was addressed both in public hearings and in the report from the US 9/11 Commission. One issue of concern was the effectiveness of information sharing by the FBI with state and local law enforcement – a problem not unique to the FBI but one common among the PS&S constituents of all jurisdictions. In part, the commission’s report stated:

³ Joel F. Brenner, *Information Oversight: Practical Lessons from Foreign Intelligence*, Center for Democracy and Technology, September 30, 2004, at page 4.

We heard complaints that the FBI still needs to share much more operational, case related information. The NYPD's Deputy Commissioner for Counterterrorism, Michael Sheehan, speculated that one of the reasons for deficiencies in the information sharing may be that the FBI does not always recognize what information might be important to others...Los Angeles Police Department officials complained to us that they receive watered down reports from the FBI. ...We have been told that the FBI plans to move toward a "write to release" approach that would allow for more immediate and broader dissemination of intelligence.⁴

Emerging theories on public safety and security indicate that the trend will be to capturing and making available more and more information to more individuals, at least in the public safety and security domain. The theories, such as "Power to the Edge"⁵ and Net-centricity⁶ advocate giving individuals at the granular or street level immediate access to as much information as possible about the risk they are dealing with, human or other.

In its August 2004 report "The Surveillance-Industrial Complex", the American Civil Liberties Union listed some of the options available to the United States government for accessing personal information.

The bottom line is that the private sector is tracking more and more of our activities for its own purposes, and the government is free to leverage this private collection as a way of extending its own powers of surveillance. The government has an array of options for accessing third-party information. It can:

- Ask for data to be shared voluntarily.
- Simply buy information.
- Demand it, using legal powers granted by the Patriot Act and other laws.
- Use laws and regulations to dictate how private-sector data is handled and stored in order to increase its surveillance value for the government.
- Create regularized systems for standing access to records of private activities.

Outsourcing becomes related to data fusion through the belief that data fusion operations — acquiring and melding databases — are easier when databases are operated by contractors within the jurisdictional range of the security agency

⁴ National Commission on Terrorist Attacks Upon the United States

⁵ Alberta et al, Power to the Edge: Command, Control in the Information Age

⁶ Alberts et al, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed., 1999, CCRP Publication Series

doing the data fusion work. It is difficult to know the extent of data-association, data-mining and data-sharing going on between government and business in North America, and to what degree outsourcing facilitates that activity. A recent journal article from American law professor Daniel J. Steinbock on “Data Matching, Data Mining and Due Process” points to 50 federal agencies using or planning to use data matching and data mining in a total of 199 programs, some of which are aimed at locating potential terrorists within the North American security zone.

Data resulting from everyday government and marketplace transactions is now bound for a new type of unintended user, the national security police analyst. As Assistant Privacy Commissioner of Canada Heather Black underscored in her findings on PIPEDA Case #313 (October 2005), in considering a complaint against a Canadian bank that contracted to an American outsource provider processing accounts in the USA, Canadian organizations are subject to similar types of orders requiring the disclosure of personal information held in Canada from Canadian authorities. Though data-fusion methods have found vocal proponents in the USA, and have been highlighted by homeland security initiatives in that country, they are bound to hold attractions for security officials in other countries where authorities have access to government and marketplace databases.

3. Current-state Review of Outsourcing Agreements

3.1 Alberta’s 2005 Outsource Agreements Survey

The “outsourcing issue” became a matter of public debate in February 2004, when the B.C. controversy sprang up from a union court challenge to the B.C. Government’s decision to outsource. It is unnecessary to duplicate the major investigation being undertaken by the B.C. Commissioner’s Office with respect to the United States’ PATRIOT Act. Our decision was made to review outsourcing generally as opposed to specifically focusing on entities subject to the UPA. This review was conducted as a joint research effort with the Alberta Government. The Commissioner’s November 2004 press release explained the scope of our joint survey project, and committed to providing an independent report to Albertans on the risk to privacy from the outsourcing of government information work.

The January 2005 Survey was conducted by Alberta Government Services under the auspices of an *ad hoc* cross-government management committee. The Office of the Information and Privacy Commissioner, as a joint sponsor of the Survey, placed a representative on the Outsource Agreements Committee.

The survey questionnaire was released in late December 2004 with a January 2005 response deadline. It was directed to all government ministries and sent as well to select local public bodies, including some major cities, universities, colleges, public and separate school boards, police services, and to all regional health authorities. All these bodies are public administration entities governed by Alberta's FOIP Act.

The rate of return on the survey was high, though some bodies requested extra time to provide summaries of their existing outsource agreements. In total, 45 public bodies submitted summary information on 134 outsource agreements in time for our analysis stage of the project.

The questionnaire asked public bodies to report on outsource agreements that put significant amounts of Albertans' personal information in the hands of contracted outsource providers. It further asked for an indication of which outsource agreements featured information storage outside Canada, including, but not limited to, the U.S.A.

The survey results (though in some sectors only a representative sample and open to discretion by public bodies as to what agreements are of 'significant' magnitude) are a good enough cross-section to allow for sector-specific observations. The following observations are a synopsis based solely on the information provided in questionnaire responses from the public bodies.

3.2 Results from Alberta Government ministries (including boards, agencies and commissions)

A total of 23 provincial government public bodies reported on 34 current outsource agreements.

Provincial Government Sector's Use of Outsource Contractors

- Some common service functions are handled for all government ministries through a single outsource agreement. For example, the IMAGIS system, built on a PeopleSoft product base, is provided by Alberta Restructuring and Government Efficiency (RGE) for use by all ministries in managing finance and human resources. IMAGIS contains personnel and banking information, including data on attendance, performance, and health benefits eligibility, for employees in the Public Service of Alberta. RGE in turn engages IBM Canada Ltd. as an external outsource provider to handle systems operations and back-end processing for IMAGIS, leaving front-end input to be done by government staff. The IMAGIS project is one example of how complex information systems are first consolidated internally through inter-

ministerial cooperation, and then outsourced externally for ongoing service delivery.

- Some larger ministries have set up overlapping outsource arrangements, where more than one outsource provider is involved in delivering the required customer value. For example, Alberta Health and Wellness, with its large healthcare databases, engages IBM Global Services (formerly ISM Alberta) to manage those assets, while also engaging CGI as the outsourcer managing IT applications that run on those databases.
- Some ministries see advantages in having their comprehensive ICT management function provided by an outsourcer, as in the case of Alberta Municipal Affairs' agreement with Fujitsu Consulting Inc. for integrated systems management services.
- Ministries rely on outsourcers for specific program support (e.g., Alberta Economic Development's use of outsourcer Advanis Inc. to deliver Travel Alberta Contact Centre services).
- In other cases, ministries use outsourcers for specialized problem-solving (e.g., Alberta Education's use of an outsource program by Education Logistics Inc. to calculate distances from student's homes to their schools for figuring out school transportation routes).

Provincial Government Sector's Approaches to Data Location:

- Data is usually housed on Government of Alberta servers. There are exceptions like the Motor Vehicles System ("MOVES"), outsourced to EDS Canada and run on that company's Markham, Ontario facility.
- The current contract for the IMAGIS system requires that outsource provider IBM keep the data in Alberta, with allowance for temporary data migration to IBM's Ontario site in cases of disaster recovery.
- Provincial healthcare data is located in Alberta, using IBM facilities in Calgary, with disaster recovery arrangements involving Ontario data centres.
- US-based outsourcers are an anomaly. The General Education Development test program offered to adult students by Alberta Education is entirely an American product, provided by GEDScoring.com, with registration and scoring data housed completely in the USA. Paternity testing activities of Alberta Children's Services and its regional delivery bodies, in which mandatory paternity-grouping DNA specimens are collected for analysis and reporting, are outsourced

to a laboratory company that moved recently from Canada to the United States. A public body wishing to outsource DNA testing faces a marketplace capacity problem in Canada. In both cited examples of data being lodged in the US, there is a value-added aspect to the outsource agreements, where the outsourcer augments the personal data by developing new results through a proprietary process. Records of the personal information data used in these transformation processes are maintained by the outsource providers in the USA.

- Government of Alberta contract management practices indicate an awareness of issues of data location and accessibility, particularly where outsource providers are subjected to mergers and acquisitions. For example, in June 2004 Alberta Advanced Education engaged the services of EDULINX Canada Corporation to provide loan disbursement, maintenance and repayment services to students who have received student loans to attend full-time post-secondary studies. EDULINX, then owned by the Canadian Imperial Bank of Commerce (CIBC), served several Canadian jurisdictions as their student loans outsourcer, managing a complex credit and banking system with large repositories of detailed personal information. In October 2004 CIBC sold EDULINX to Nelnet Canada Inc., a subsidiary of a major American student loans corporation based in Nebraska. In January 2005 the Minister of Advanced Education amended his contract with EDULINX Canada Corporation to ensure that the Minister's data is located only in Canada and that all data collection, processing, transactional and archiving entries operated or contracted by EDULINX is located only in Canada. The amendment went further, ensuring the data is accessible only in Canada and that the data is kept physically independent, both directly and indirectly, from any databases located outside Canada. In signing off on the amendment, EDULINX agreed that it must comply with provisions of the agreement notwithstanding any conflicting law of any jurisdiction outside of Canada which may purport to override Canadian privacy laws.

Provincial Government Sector's Outsourcing Agreements

- There is a wide variation in approaches taken to auditing provisions in outsourcing agreements. Formal audit schedules (where public bodies require cyclical audits or reports on systems testing) are rare, except in agreements covering the very large systems. Most agreements include an audit prerogative for the public body, covering not only audit of processing but also audit of the outsource provider's books, statements, accounts and records, including access to the outsource provider's employees. Large programs in which data is kept at the outsource provider's site contain provisions allowing the public body to conduct

on-site visits, inspections and investigations. In some cases, charges for audits by the public body are to be borne by the contractor. The right to name the auditor is sometimes explicitly reserved for the public body. While some smaller programs show no audit provisions, they tend to be agreements that can be terminated without cause after a short (30 day) notice period.

- Agreements regularly feature prohibitions on use and disclosure of information. The large health-care agreements require the outsource provider to maintain individual employee user access logs. The model security and confidentiality clauses used in the major agreements cover the eventuality of unauthorized copying, requiring that it be investigated and reported.
- Some agreements stipulate financial consequences for data loss or for breaches of confidentiality. In those agreements, loss of data is scheduled as a 'service measure' liable to a specific deduction being assessed against the annual service charge to be paid to the contractor, with even more severe penalties for failing to report the loss within a stipulated period (e.g., 24 hours).
- Outsource agreements in the sensitive information areas of child welfare and income assistance routinely contain provisions that require the Minister's written consent in advance of any disclosures of information by the outsource provider.
- The agreement covering motor vehicle information explicitly denies any claim by the contractor to a proprietary right to the information. It also includes detailed requirements for the return of all information on conclusion of the contract. The contractor must also advise the public body within 24 hours of any changes to the location of the records.
- Injunctive relief clauses are fairly standard, allowing the public body to immediately suspend the contract if a privacy breach is shown, without having to prove harm.
- Government ministry outsource agreements treat a breach of confidentiality as constituting a material breach of the contract, subject to contract termination with little or no curing period.

3.3 Results from municipal government and police services sectors

A total of 4 municipal government public bodies reported on 42 current outsource agreements. A total of 3 police service public bodies reported on 2 current outsource agreements.

Municipal Government/Police Services Sector's Use of Outsource Contractors

- The municipal governments participating in the Survey reported numerous special purpose outsource arrangements, ranging from disaster investigations (e.g., flood damage documentation) to public lands management (including cemetery plot allocation), enumerations, utility customer accounts data , and household and commercial surveys.
- Police services tend to own and run their own systems, whether as a firewalled single user or as a subscriber to a police services network. Outsourcing is used for administrative work resulting from law enforcement actions (e.g., for enforcement follow-up to ticketing and for records storage).
- Highly sensitive services such as account collections call centres and public transit for disabled persons are also outsourced to specialist providers.

Municipal Government/Police Services Sector's Approaches to Data Location:

- Outsource contractors used in this sector are generally located within the municipality. For these local companies, location of data is assumed to be confined to a desktop application at the contractor's site. However, it is not clear from the questionnaire responses that local contractors are not using outwardly-linked software to support their local operations.
- A close examination by the City of Edmonton of its 25 outsource agreements indicated that 11 (44%) kept the information in Edmonton, while 7 stored it in Ontario, 2 in British Columbia, 2 in Saskatchewan, and 1 each in Manitoba and in Quebec. Only one agreement placed information outside Canada, that being a Massachusetts-based IT service contractor performing test work on the Mobile Data Computer System that supports Edmonton's DATS public transportation service.

Municipal Government/Police Services Sector's Outsourcing Agreements

- The municipal agreement summaries reviewed contain no provisions for monitoring or auditing the contractors.
- Many outsourced applications involve employee data (e.g., employee service recognition programs).
- Some special purpose outsource arrangements are not covered by express contract (e.g., municipal EMS branch using unsigned outsource contractor to provide incident data to Alberta Health and Wellness).

3.4 Results from the public post-secondary institution sector

A total of 5 public post-secondary-institution public bodies reported on 10 current outsource agreements.

Post-secondary Sector's Use of Outsource Contractors

Alberta's universities, colleges and technical institutes use and contribute to international information-sharing systems, including many specialized North American learning networks. A number of functions are outsourced, including library subscription services, alumni and foundation databases, employee wellness and benefit programs and corporate credit card services.

The learning enterprise systems used in universities include reader services based in other countries, including the U.S.A. Reader services track the interests of a licensed user (a student or professor) to alert that user to the presence of new work happening elsewhere on the target topics.

In some cases universities have set up incorporated foundation databases in other countries to assure tax advantages to donors. There is also the presence of an 'alumni offer' database operating as a joint-venture outsource operation between a university and MBNA Mastercard, with enrollment and usage information managed wholly in the U.S.A.

Post-secondary Sector's Approaches to Data Location:

Concern for data location is evident in some returns to the Survey. One institution cited a concern over how outsource insurance plan administrators refer health information of applicants for optional life insurance coverage to the World Wide Assist program, now owned and operated by LabOne, Inc., the Kansas City company that describes itself as the leading provider of risk assessment testing for insurance companies in the United States and Canada.

Post-secondary Sector's Outsourcing Agreements

Public post-secondary institutions enter outsource agreements to provide the members of the institution (students and staff) with services designed for the academic sector. In some cases those services take the form of software products holding demographic/population data housed on the institution's own servers but serviced by US-based vendors (e.g., integrated library management systems). While engagement contracts between the institutions and the providers do in some cases explicitly commit to observing the rules of the FOIP Act, subsequent individual user agreements signed by students or staff are on the provider's own standard consent forms, which usually make no mention of privacy laws but do mention company privacy policies.

3.5 Results from the K-12 schools sector

A total of 3 school-district public bodies reported on 7 current outsource agreements.

School Sector's Use of Outsource Contractors

School districts collect and generate quite diverse sets of personal information, including third-party assessments, immigration data and financial data. As much of the information moving from families and assessment professionals to schools is paper-based, storage is an area of demand for outsource services.

School Sector's Approaches to Data Location

Examination of access and confidentiality provisions in a storage contract between a major school board and a large US-based international storage company finds that the storage company has not limited its activities to any particular territory and has left open its ability to comply with a subpoena without informing its client, if such secrecy is required by the issued subpoena. Canadian representatives of the company have shown that the records themselves are held in automated warehouses in Canada and do not cross any national boundaries. However, the data systems that keep and find location coordinants for the boxed records are operated from servers in the U.S. (This same situation applies to Alberta Government records in storage, maintained by the same outsource provider.) Here the risk is limited to how much personal information is used in the electronic file index titles by the client public body itself.

School Sector's Composition of Agreements

Agreements are on vendor-generated standard contracts with general confidentiality clauses, where the focus is on denying liability and establishing

nominal values for tangible stored record items in case of loss (e.g., fire or flood damage).

3.6 Results from the health-care sector

A total of 7 regional-health-authority public bodies reported on 39 current outsource agreements.

Health-care Sector's Use of Outsource Contractors

- This sector, made up of the regional health authorities (“RHAs”) and the Alberta Cancer Board, may be the most reliant on using outsourcers. The sector regularly enters agreements for vendor software maintenance and assistance that have an outsource aspect to them. One RHA reported two dozen such agreements as notable outsource situations. Another RHA of equal size found that it had no agreements rating the “significant” description.
- Outsource agreements are common in support of demographic and diagnostic databases, workload management systems, and assisted living services.
- In some cases, outsourcers are “affiliates” under Alberta’s *Health Information Act*, thereby falling under that law’s specific access and privacy rules.
- Outsource agreements cover a wide arrange of routine activities, including transcription services, operating room scheduling, home care tracking, and a host of functions relating to the accommodations services side of medical care (e.g., TV rental agreements).

Health-care Sector's Approaches to Data Location:

- Every outsource agreement described in the survey responses for this sector reported that the personal information in each system is housed in Canada.
- It is not unusual for software maintenance agreements to be with companies located in other parts of the world. The normal mode for servicing outsourced functions of ICT systems is by remote dial-up access, where a technical expert from the company will temporarily log into the computer application to check out a performance issue. During the service and testing interruption, patient databases are accessible to the technical expert at the company’s base of operations.

Health-care Sector's Outsourcing Agreements

- Audit requirements and contractor penalties are not evident in the summary reports on this sector's outsource agreements. The exception to that is for agreements for patient demographic systems, which sometimes carry audit provisions.
- In outsource agreements for direct provision of medical services (e.g., contracted dentistry services), the solution available to the RHA in a breach of contract situation is straightforward injunctive relief. Breaches of confidentiality by the outsourcer are treated in some agreements as grounds for contract termination.
- It is not clear from the summary descriptions that breaches of privacy by the outsource contractor are seen to constitute material breaches of contract in this sector. A notable feature of special purpose agreements in this sector is the tolerance for the prospect of privacy breaches happening, sometimes demonstrated by recognition in contract of a 15-30 day grace period to cure the cause of the breach.

3.7 General observations from the 2005 Survey

The outsourcing of large databases of public records for the performance of a program delivery function for an Alberta public body is usually accompanied by a formal agreement specifying that information is to remain in Alberta or Canada. There exists beyond those big agreements a number of relationships between public bodies, other public bodies and private sector contractors where the provision of services requires the flow of personal information to the private-sector service provider.

Many of these arrangements have a long history, and many are managed with a high degree of trust to the private-sector provider, based on consistent performance of the outsourced function. Some outsource arrangements grew up as break-away government-sponsored enterprises, and occasionally these are owned or staffed by former employees or officials of the public body. The survey results suggest that at least a few outsource arrangements for specialized services in local public body sectors are not supported by documented contracts or are based on contracts which do not fully address and secure the access and privacy obligations and risks of the public body.

From the range of returns provided to the January 2005 Survey, it seems that it is no longer clear what the term "outsource" means for public bodies. Many functions once performed in-house are now so routinely "outsourced" that they are no longer counted as natural functions of a public body. Examples include cheque production, payroll and pension administration, ICT systems support, security services, mail systems, billing production, account statements,

employee counseling, call centre representation, and even basic telephone reception.

Subcontracting by outsourcers is a concern. A public body having a contract with an outsource partner has a direct, legal relationship with that partner. They are aware of the contractual rights and remedies and are in a position to exercise them directly vis-à-vis their contracted partner. Furthermore, a public body can choose who to contract with, exercising whatever due diligence it deems necessary in making the selection. This is not necessarily the case with sub-contracted outsourcers. The principle contracted outsourcer may choose its subcontractors based on entirely different criteria than would the public body. A breach of the sub contract may only be actionable by the contractor; the public body may have no ability to deal with the subcontractor except through the principle contractor. The summary responses to the January 2005 Survey do not provide sufficient detail to determine whether proper checks and balances are in place to preserve the public body's interests where sub-contracting by outsourcers occurs.

The unevenness in establishing audit requirements is a common observation across all sectors. Formal audit provisions have not been a standard requirement for government contracts.

A complication for public bodies outsourcing to companies that keep continental or worldwide databases is the presence of some identifiable personal information in other jurisdictions. This appears in several records storage agreements for major public bodies, where the stored record remains in Canada (usually within a short retrieval range of the client public body) but where file locator index information resides outside Canada. Further examination of whether that file locator data actually discloses any personal information to foreign-based systems operators should be undertaken by the records management programs within public bodies.

4. Strategies to Mitigate Risk and Improve Privacy

4.1 The range of measures to consider

The B.C. Commissioner made 16 detailed recommendations to address the particular question of the UPA's implications for outsourcing of provincial government programs, suggesting 32 actions and practices from both a provincial and national perspective. The British Columbia Government passed its Bill 73 reforms ten days ahead of the final report being issued by the Commissioner in October 2004. The Bill reformed the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and went part way to anticipating the

recommendations, adding some measures not explicitly addressed in the Commissioner's report. The new legislative rules make it a provincial offence for service providers to:

- Store, access or disclose personal information of a B.C. public sector body outside of Canada (although there are narrowly defined exceptions);
- Fail to provide notice to the Minister of Management Services of any foreign demand for disclosure of personal information held by the service provider; or
- Discipline, suspend, demote, harass or otherwise disadvantage an employee who, acting in good faith and on the basis of reasonable belief, complies with the notice obligations or acts to insure compliance with FOIPPA.

The maximum penalty for non-compliance is a fine of \$500,000.

The B.C. Government's decision to apply moderate penalties to its reforms of the FOIP Act may be an issue when the magnitude of those sanctions comes to be considered by a foreign court. The magnitude of the penalty may be seen as an indication of importance by the Canadian jurisdiction.

The practical implications of Bill 73 have appeared in post October 2004 contracts between B.C. public bodies and outsource providers ("OPs"). Among new features appearing in B.C. contracts are:

- requirement for segregated data access,
- requirement to keep individual user logs,
- non-disclosure agreements (between individual OP employees and the public body itself, between employees of an OP's sub-contractor and the OP, between employees of the OP's sub-contractors and the public body itself),
- annual oaths to be taken from employees of the OP and employees of the OP's sub-contractors,
- procedures to restrict the actions and access of foreign-based employees working on transition and transformation activities,
- limitations on data access, including data remote access,
- corporate internal limitations on data access, cutting off extra-provincial access,
- alarm notification facilities to alert the public body to copying or unusual access activity,
- prohibitions on OP staff outbound web and email access,
- restrictions on data portability hardware (CD burners, USB smart drives, etc) to just designated personnel,
- dedicated OP privacy officers to monitor compliance,

- financial penalties in contract in event of disclosures or privacy breaches.

Some major post-October 2004 service providers to the B.C. government have created provincially-incorporated subsidiaries to manage new agreements within the constraints of Bill 73. Some pre-existing service providers are now in the process of changing their worldwide, continental, and national data management architecture to effectively segregate information holdings. Some outsource providers are exploring ways to leave Canadian data physically located in another country but in an encrypted manner where the keys to unlocking the personal information in the data are kept in the control of the Canadian subsidiary to the foreign-based company.

The changes coming out of British Columbia as a result of Bill 73 have yielded some unintended consequences, as we understand that public bodies are experiencing disruptions in ICT routines (e.g., access to data by staff on assignment outside the province). Some of these unintended consequences were addressed by amendment to B.C. FOIPPA in October 2005. The amended legislation prohibits the storing, accessing or disclosing of personal information outside of Canada. Suppose the back-up or help desk for the software being used by an entity in Canada is in another country. In order to provide help or troubleshoot a problem, the help desk needs to see the file which presents the problem. If the user in Canada allows the help desk in Guatemala to view that particular file and the file contains personal information, that is likely a breach of the B.C. Act. It is sometimes the case that this kind of outsourced service provider has the ability to access personal information in Canada, but would normally only do so as needed, on a case by case basis. In some cases, it may be that the help desk function could be located in Canada. The question becomes whether the function can be located in Canada at a reasonable cost, while still providing an acceptable level of service. For example, health records systems might require a 24/7 helpdesk. This may not be available in Canada. Does the need for 24/7 service justify the risks presented by foreign outsourcing? Further, in the case of highly specialized software, there may only be one help desk in the world. Therefore, adoption of similar recommendations and emulation of similar statutory reforms should not be implemented in Alberta without researching and observing the B.C. experience.

The Alberta Government's Outsource Agreements Committee, responsible for administering the January 2005 survey, is developing its own recommendations to the Government. The Outsource Agreements Committee has recommended revisions to the FOIP Act to establish strict controls over the ability of public bodies to disclose personal information to foreign courts or pursuant to orders of foreign courts.

OIPC is of the view that the most effective control and governance of outsourcing will require a mix of statutory provisions, enhanced diligence in the

selection and monitoring of contractors, rigorous application of model contract formulations, and transparent testing and audit programs. The goal is to reduce the risk of disclosure to unintended users. Given what we have seen in complaint investigations involving outsource providers and in our look at the state of current outsource arrangements in Alberta, the Office of the Information and Privacy Commissioner supports a strategy of acting on all fronts (legislative, contractual, and operational) to contain risks.

Our analysis does not take us to the step of recommending an expansion of the scope of the FOIP Act to make outsource providers directly accountable and subject to the Commissioner's powers of investigation and the Commissioner's binding order-making authority. The current accountability structure in Alberta's FOIP Act, wherein it is the public body that carries the full responsibility for compliance with FOIP, and wherein all records in the control of a public body are subject to the Act, regardless of whether they are in the possession of the public body or a contractor, is an appropriate structure.

We are mindful that, since the coming into force of PIPEDA, and the similar provincial private sector laws in Alberta, B.C. and Quebec, most private sector organizations in Canada are regulated with respect to the collection, use and disclosure of personal information.

On the question of data location, risk analysis points to broad demographic government databases as being of greatest interest to unintended users. These databases (e.g., health care, motor vehicles, student loans) are outsourced by arrangements that already keep them within Canadian boundaries. It would be possible to reinforce the status quo by legislating the requirement that data be kept in Canada. However, such a requirement would have to be very precisely worded; too broad a restriction could result in serious disruption of business or worse, disruption of critical services. The occasional flow of low-risk information bits across borders is important to the smooth operations of some public body programs. Though individual medical patient information in particular is highly sensitive in its own right, the minute amounts within special purpose systems may not be viewed as a significant risk. Exceptions must be allowed for the movement of medical information to other parts of the world where specialist consultants require it to provide the contracted medical support service.

The following recommendations then are a synthesis of the Office of the Information and Privacy Commissioner's

- analysis of the January 2005 Survey and public-body practices;
- experience in investigating breach of privacy situations involving outsource agreements;
- observation of legislative developments in British Columbia and consideration of the conclusions reached by the BC Commissioner;

- assessment of the current state of policy on public-sector outsourcing in Alberta; and
- assessment of opportunities in existing legislation to provide greater assurance that the risks presented by outsourcing are being mitigated.

4.2 OIPC recommendations for Alberta Government action

Legislative

It is important that the Government make a strong and unequivocal assertion of the value it places on the privacy and security of the personal information of Albertans. This does not need to extend to a complete ban on foreign disclosures.

1. Amend applicable legislation (i.e. Freedom of Information and Protection of Privacy Act) to clearly define responsibility for outsourcing personal information. The onus for due diligence in outsourcing should be clearly placed on the outsourcing organization (i.e. the public body).
2. Amend section 40(1)(g) of the Freedom of Information and Protection of Privacy Act and section 35(1)(i) of the Health Information Act⁷ to make it clear that personal information can only be disclosed pursuant to an order of a Canadian court having jurisdiction.
3. Increase the penalties for breach of the FOIP Act and the HIA.
4. Ensure that the offence provisions of the FOIP Act and the HIA can be reasonably sustained, that is, the standard is not so high as to preclude a reasonable chance of conviction. The current standard is “willful”.
5. Consider the advisability of making similar amendments to the Health Information Act.

Contractual

First, there should be a checklist or template of matters to be considered in making the decision to outsource. This could be done via a privacy impact assessment. Secondly, develop a model outsourcing contract and a checklist of contractual provisions to be considered in outsourcing arrangements. Such contract or checklist should address at least the matters referred to in sections 2.3 and 4.1 and should include provisions dealing with:

⁷ It is noted that, under the HIA, “custodians” are responsible for collection, use and disclosure by their “affiliates”: section 62. “Affiliates” are required to collect, use and disclose only in accordance with their duties to the custodian: ss 24, 28, 43. Furthermore, section 8 of the Regulation to the Health Information Act (AR 70/2001) reproduced as Appendix Z, contains a good test of considerations with respect to the security of health information. Subsection 4 contains five matters that must be dealt with in written agreements between custodians and “outsourcers” outside of Alberta.

6. A prohibition on assignment or subcontracting of the outsourcing contract without written consent.
7. A requirement for notification by the outsourcer in the event of notice of creditor's remedies or Court applications for bankruptcy or protection from creditors.
8. A requirement of notice on any demand for access to or disclosure of personal information received by the outsourcer.
9. A requirement of notice of any loss of or unauthorized access to personal information by the outsourcer or its employees.
10. Right to audit, not only for compliance with the contract but compliance with any legislation stipulated to be applicable to the contract.
11. In addition to the right to audit, the outsourcer may be required to have in place a system which monitors or audits the outsourcers' use and disclosure of the personal information. The outsourcing entity may require access to those logs on certain conditions.
12. Stipulate consequences for breach. In addition to right of termination and damages, provision should be made for: return of personal information and any copies of it; assistance in recovering lost or otherwise disclosed personal information.

Policy/Operational

13. Retain, as a first principle, that personal information only be outsourced within Alberta first, Canada second, and anywhere else third, depending on the specific circumstances. This policy may only be deviated from where the requirements of program delivery, such as cost, service, security, cannot reasonably be met within Alberta or Canada. The outsourcing organization should bear responsibility for making this decision and for the consequences of having made it. Whether to make such policy into law poses a dilemma, as discussed. As stated, the decision to outsource is based on a large number of factors. The decision to outsource outside of Canada requires reconsideration of these factors in light of the fact that the public body is that much more removed from the outsourcer:
 - Different laws;
 - Different customs (are laws pertaining to fraud, theft of information and so on regarded or enforced differently?)
 - Different workforces (are the outsourcer's employees more transient, less reliable, more difficult to hold accountable, etc.?)

The gains realized from outsourcing have to be weighed against the risks presented by the nature (sensitivity, value) and the volume of the information outsourced.

14. Require preparation of a privacy impact assessment (which would include issues of security) for all outsourcing arrangements involving “significant” amounts of personal information. We debated recommending that this be put into law. Legislated provisions can be inflexible. For example, it would not make sense to prepare a privacy impact assessment every time a single sample of genetic material is sent to another country for analysis.
15. Require outsourcing organizations to keep a master list (inventory) of outsourcing agreements. This could be accomplished by requiring privacy impact assessments. This list should be accessible to the Chief information/Chief Privacy Officer for the public body. The purpose of the list is to: know what personal information is outsourced where and to who; enable timely action in the event that the outsourcee becomes insolvent; and to enable agreements to be updated when they end to include state of the art privacy and security provisions.
16. Someone in the public body must be specifically responsible for each outsourcing agreement. This person should know the outsourcer and the contract. There should be regular contact, check ups, and queries. Scheduled or spot audits may be advisable.
17. With respect to foreign outsourcers, consider having a trusted agent in the jurisdiction to monitor social/legal developments respecting the outsourcer.

4.3 Commissioner's conclusions

Information Communication Technology (ICT) outsourcing has become a mainstream service delivery strategy for public bodies in Alberta. Through generally cautious management and policy foresight, information resources entrusted to Alberta public bodies are for the most part secure within Alberta or Canada and not exposed to unintended users in foreign jurisdictions.

The ICT outsource industry is made aware of Alberta's access and privacy law requirements through express contract language and through interaction with public body administrators.

The position of Canadian ICT outsourcers linked to US-based companies remains unclear and would benefit by reinforcement in law and in model contract provisions. These improvements to legal and contractual frameworks should be matched by more rigorous attention to outsource agreements management by public bodies which choose to use them.

<<<<<<<<< >>>>>>>>>>>>

Appendix A: Literature Review on Outsourcing

This literature review explores critical aspects of public sector outsourcing through academic research. It aims at answering two questions: What is outsourcing? and Why does the public sector engage in this practice?

This literature review is a sampling of research covering outsourcing (contracting out) of government services in general. The scope of the review

was focused on academic research papers about outsourcing of government services. Despite the lack of research directly related to Canadian experiences, the following works provide helpful frameworks for understanding outsourcing in the Canadian context.

Barrett, Pat. "Contract Management and Accountability" Australian Journal of Public Administration. 60(2) (2001) 123 – 124.

This short article authored by Barrett, Auditor General for Australia, focuses on contract management and government accountability. Barrett's bottom line is that accountability cannot be outsourced and any contract must specify the services required; the relationship between the parties needs to be clearly defined; and appropriate arrangements for monitoring and reviewing contactors' performance need to be outlined. The author does warn, however, that in a world with increasing development of networked systems, a change in the dichotomy of contractual obligations will occur. Barrett concludes by noting the release of a publication from his office designed to assist governments with outsourcing: *Better Practice Guide on Contract Management*.

Brown, T.L. and Potoski, M. "Contract-Management Capacity in Municipal and County Governments" Public Administration Review. 63(2) (2003) 153 – 165.

Brown and Potoski examine contracting out of services in the municipal and county governments context and focus the discussion on how governments' managerial capacity may improve contract performance and may also explain why some contract arrangements are more successful than others. The authors divide their paper into eight sections: literature review in the field of government contracting and contract management, definition of contract-management capacity, factors that create the need to invest in capacity, hypotheses on why governments invest or not to invest in contract-management capacity, test of the hypotheses, results, discussion on the implications of the results, and finally, discussion on the implications of the findings. Brown and Potoski conclude that governments invest in contract-management capacity when previous contracting experiences support higher investments, when transaction costs are high, and when internal and external factors favour the investment. The authors assert that shortcomings and problems associated with contracting-out of services can be alleviated to some degree when governments respond to poor conditions by investing in the managerial capacity to identify suitable situations for contracting, to negotiate strong contracts, and to monitor vendor performance.

Butler, Michael J.R. “Managing from the Inside Out: Drawing on ‘Receptivity’ to Explain Variation in Strategy Implementation” British Journal of Management. 14 (2003) S47 – S60.

Butler discusses the rise of “New Public Management” or NPM as government policy used to facilitate public sector outsourcing and downsizing. The paper draws on the concept of “receptivity” for organizational change to explain the variation in strategy implementation. Receptivity is an idea that attempts to determine the factors that lead to organizations being low-change, non-receptive contexts or high-change, receptive contexts to outsourcing. Receptivity was used to explain the success of two contrasting English local housing authority outsourcing strategies. In the first local housing authority, external private-sector contractors were not used, while in the second they were. Butler identified four receptivity factors to explain the two contrasting outsourcing strategies: ideological vision, leading change, institutional politics and implementation capacity. He concluded that although organizational change may be created differently in the two local housing authorities, the process of change may be similar as illustrated in the four receptivity factors. Overall, Butler’s analysis of the receptivity factors provided a good overview of how some organizations are more receptive to change than others.

Cohen, Steven. “A Strategic Framework for Devolving Responsibility and Functions from Government to the Private Sector” Public Administration Review. 61(4) (2001) 432 – 440.

Cohen works from the premise that a government organization performs a function, but must decide on whether that function should be carried out by government or indirectly, through the use of a non-government organization. His work is primarily about privatization, but does contain insights about making outsource decisions. The author’s paper is divided into two sections: first, identifying the distinguishing characteristics of government, non-profit, and private sector organizations, and assessing how these characteristics impede or facilitate the performance of a set of typical public functions. The second section of the paper develops a framework and a method for making such decisions. Finally, Cohen identifies a strategic framework for making the privatization decision and applies this framework to the case of privatizing homeless services in New York City. Cohen identifies three theoretical approaches to outsourcing which are interesting from an institutional point of view and may be of some benefit to the government manager responsible for the outsourcing

decision. The author concludes that government managers should resist bias and easy assumptions in making the outsourcing decision. Cohen recommends a strategic approach to privatization where traits such as political, economic, social, technical, and ethical issues be addressed prior to making the outsourcing decision.

Eggers, William D. "Networked Government" Government Executive. 35(8) (2003) 28-32.

The opening sentences of Eggers study succinctly foreshadows his subject matter: "It's not about outsourcing vs. bureaucracy. It's about managing diverse webs of relationships to deliver value." Eggers' argument is that the traditional organizational model is based on a hierarchical government bureaucracy that is being forced to adapt to society's complex needs. As a result, government executives are redefining their core responsibilities from managing people to coordinating resources for producing public value. Eggers focuses on U.S. Federal Government outsourcing experiences from differing department and agency perspectives supplemented by specific outsourcing experiences in New Zealand and the United Kingdom to strengthen his argument. Although this is a relatively short article, Eggers does a good job of identifying the move from a hierarchical organizational model to a network model which in his opinion is a model better suited for outsourcing.

Jorgensen, T.B. and Bozeman, B. "Public Values Lost? Comparing cases on contracting out from Denmark and the United States" Public Management Review. 4(1) (2002) 63 – 81.

The authors take the perspective of values when examining the issue of contracting and outsourcing, specifically they focus on the public value system and the extent that values are taken into consideration prior to contracting. Values presented include: political accountability, regime stability, transparency, social cohesion, user orientation, and efficiency. By exploring three case studies on contracting out, one in Atlanta, Georgia and two in Denmark, the authors attempt to answer the question: "To what extent and in what ways are public values taken into account in decisions about contracting out?" Jorgensen and Bozeman identify a long list of values gathered from literature on public management before launching into their case studies. The identified values help frame the case studies and assist in answering the authors opening question. Jorgensen and Bozeman conclude that contracting out, in some instances, seems to threaten public values but does not require governments to abandon them. Overall, this is a well-written

and researched paper which allows readers to extrapolate the frames used in this study and apply them to their own organizations.

Schmid, Hillel. "Rethinking the policy of contracting out social services to non-governmental organizations" Public Management Review. 5(3) (2003) 307 – 323.

As the title of this paper indicates, Schmid examines the utility or "rethinking" of contracting out social services to non-governmental organizations. In particular, Schmid focuses on the contracting out of services such as foster care, adoption and home care services for the elderly in the Israeli scene. Examining relevant literature to the study of contracting-out of services, the author notes that governments are guided by ideological and utilitarian considerations for adopting the strategy of outsourcing. From an ideological point of view, some governments believe that contracts "enhance both efficiency and accountability because they combine market competition with a more rigid performance control system."(308) From a utilitarian perspective, Schmid indicates the research is less conclusive due to "diversity of funding sources, disparate organizational goals, varied constituencies and variety of clients"(310). The author's examination of contracting out in Israel is thorough and well-presented and at the end of the paper offers five intriguing conclusions. First, governments have relieved themselves of the burden of service provision yet broadened the scope of services offered. Second, non-government organizations serve as buffers and mediate between the government and clients. Third, as the main provider of resources to government, non-government organizations lose their advantage of operative flexibility and rapid response to the needs of clients because government forces them to conform to its norms of bureaucratic behaviour. Fourth, there is a risk that clients will not receive the services entitled to them because the government relieved itself of its responsibility to provide such services while non-government organizations often seek to make a profit. Finally, the transfer of responsibility to the non-government sector may result in greater inequality and social and economic gaps between clients.

Zifcak, Spencer. "Contractualism, Democracy and Ethics" Australian Journal of Public Administration. 60(2) (2001) 86 – 99.

Zifcak examines contractualism and the process where functions once undertaken by government are now performed by private or voluntary organizations in a contractual relationship with public service departments and agencies. Specifically, he looks at contractualism from a democratic perspective analyzing the process as it relates to certain

core political values: transparency, probity, and public deliberation. Zifcak cites a number of researchers who are specialists in the field of public management and communications. There are also detailed examinations of the three core political values and how they intertwine with outsourcing. In particular, Zifcak notes that outsourcing “presents significant challenges for the maintenance of high standards of probity.” He concludes that market forces may be a better mechanism for the distribution of certain goods and services but they seem to be less suited in addressing distribution of rights and entitlements (i.e., whether policies are just or unjust, equitable or inequitable, coercive or non-coercive).

Overall, the selected articles neither praise nor condemn outsourcing as an organizational tool. Rather, the authors prescribe means to reduce the risks associated with outsourcing, identifying lack of institutional accountability once the outsourcing contract is in place as a major source of risk.