SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT F-2013-001

Public Service Commission

Summary: In 2009, a skills survey was distributed to Government of Saskatchewan employees. The Office of the Saskatchewan Information and Privacy Commissioner received a letter from staff of a government institution outlining concerns over how the personal information collected from the skills survey would be stored in the United States of America (USA) and therefore subject to the *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA PATRIOT Act). The letter also indicated that the Public Service Commission (PSC) Careers website, that lists job postings for the Government of Saskatchewan, is also hosted in the USA. The Commissioner undertook an investigation pursuant to section 33 of *The Freedom of Information and Protection of Privacy Act* (FOIP). He found that PSC had insufficient safeguards to protect personal information it collected through the skills survey and the PSC's Careers website. The Commissioner recommended that: (1) PSC clearly determine and document its own security standards and practices; (2) that PSC make amendments to its contract between it and its service provider; (3) that PSC undertake a privacy impact assessment to ensure it is in full compliance with FOIP and *The Health Information Protection Act*. He also recommended that PSC provide clear notification to all employees and job applicants that, without an explicit duty to protect provision in FOIP, there is inadequate protection of personal information and personal health information when it is released to a private contractor.

Statutes Cited: *The Freedom of Information and Protection of Privacy Act,* S.S. 1990-91, c. F-22.01, ss. 5, 24, 28, 29, 31(1), 32, 33, 49(2); *The Health Information Protection Act*, S.S. 1999, c. H-0.021, s. 16; *The Local Authority Freedom of Information and Protection of Privacy Act* S.S. 1990-91, c. L-27.1;

Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5; British Columbia's *Freedom of Information and Protection of Privacy Act* [RSBC 1996] c. 165, s. 30.1; Alberta's *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25, s. 40(1)(g); Alberta's *Personal Information Protection Act* S.A. 2003, c. P-6.5, s. 13.1; Nova Scotia's *Personal Information International Disclosure Protection Act*, Chapter 3 of the Acts of 2006; Ontario's, *Municipal Freedom of Information and Protection of Privacy Act* R.S.O. 1990, c. M.56; United States of America's *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* Public Law 107-56 115 Stat. 272 (2001).

Authorities Cited: Saskatchewan OIPC Review Report LA-2010-002; Investigation Reports H-2011-001, F-2012-001; Alberta IPC Order F2010-023; Ontario IPC, Order MO-2770; OPC PIPEDA Case Summary #2005-313.

Other Sources Cited: Saskatchewan OIPC, *2003-2004 Annual Report*, *2004-2005 Annual Report*, *2005-2006 Annual Report*, *A Contractor's Guide to Access and Privacy in Saskatchewan*, January 2006 *Saskatchewan FOIP FOLIO*, February 2006 *Saskatchewan FOIP FOLIO*; Alberta IPC, *Public-sector Outsourcing and Risks to Privacy*, February 2006, *Privacy and the USA PATRIOT Act: Implications for British Columbia Public Sector Outsourcing*, October 2004; British Columbia Government, *Privacy Protection Schedule*; British Columbia IPC, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*, *Guidelines for Data Services Contracts: OIPC Guideline 01-02*, May 8, 2003; Ontario Information and Privacy Commissioner, *Privacy Investigation Report PC12-39: Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report*, June 27, 2012; OPC, *Annual Report to Parliament 2004-2005: Report on the Privacy Act*, *Processing Personal Data Across Borders Guidelines*; Provincial Auditor of Saskatchewan, *2011 Report – Volume 2*; Government of Saskatchewan, *An Overarching Personal Information Privacy Framework For Executive Government;* Saskatchewan Justice Access and Privacy Branch, *Personal Information Contract Checklist, Version 2.2*; Legislative Assembly of Saskatchewan, Board of Internal Economy, *Hansard Verbatim Report*, February 5, 2013; Government of Alberta, *FOIP Bulletin No. 18, Managing Contracts under the FOIP Act*.

Table of Contents

I BACKGROUND

[1] In September 2009, my office received a letter from an employee of a government ministry (Ministry A) that stated staff were concerned with an employee skills survey that they were asked by their Deputy Minister to fill out. This was confirmed by the Privacy Officer of Ministry A who indicated that other employees had also expressed similar concerns with the practice. The staff's concern surrounded how information collected by another government ministry, the Public Service Commission (PSC)[1], through the employee skills survey and the job application process would be stored in the United States of America (USA).

[2] PSC explained to my office that the information gathered from the survey was to be used for redeployment purposes in case of a "significant event (such as a flu outbreak)".[2] Information sought by the survey included the employee's current work duties, past work assignments, their full name, employee number, place of residence, work headquarters, e-mail address, home phone number and cellular phone number.

[3] It came to my office's attention that the survey was being hosted by a USA-based company, offering an array of Information Technology (IT) services (Company X), and that the information would be subject to USA laws including the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA PATRIOT Act).[3]

[4] As exemplified by Ministry A's staff, there are significant concerns with individuals providing their personal information to their provincial government only to become subject to the laws of another jurisdiction such as the USA. Throughout this Investigation Report, I will discuss the recommendations that I have made to address

[1]The information was collected by the Public Service Commission (hereinafter PSC). Through a government reorganization, PSC was moved into the Ministry of Central Services at one point while the review was underway but PSC has remained a "government institution" throughout.
[2]PSC submission to the Office of the Saskatchewan Information and Privacy Commissioner (hereinafter SK OIPC) dated February 28, 2012.
[3]United States of America, *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (hereinafter USA PATRIOT Act) Public Law 107-56 115 Stat. 272 (2001).

such concerns. My recommendations include: 1) legislative reform to *The Freedom of Information and Protection of Privacy Act* (FOIP)[4] that will impose upon public bodies the duty to protect personal information in its possession or control, 2) significant fines and/or imprisonment for non-compliance with the aforementioned duty to protect, 3) that "personal information" as defined by section 24 of FOIP is treated in accordance with Part IV of FOIP, and that public bodies recognize it is unique from other types of information, 4) contracts between public bodies and contractors must stipulate that there will be no assignment of the contract or subcontracting without prior approval from the public body, and 5) contracts must stipulate that contractors must comply with FOIP when they are carrying out responsibilities under the contract with the public body.

[5] In regards to this specific case, Ministry A's staff concerns were addressed in part when its Director, Legislative Services and Privacy advised my office of the following:

> As you are aware some employees from our ministry raised concern with your office with completing and submitting a skills inventory form to be used for pandemic planning as they understood the PSC stores the information on a server located in the USA, making it potentially accessible to US government authorities under The Patriot Act. We have since had some discussions with the PSC and the employees have been advised to complete the form but rather than send it to the PSC to send it to the ministry's emegency [sic] planning officer to retain for possible future use in the ministry's pandemic planning...[5]

[6] It appeared that employee information from government institutions other than Ministry A, were also being collected and stored in the USA. This includes job applicants' personal information collected through the online job application process.[6] My office advised PSC by way of a letter dated October 27, 2009 that we were undertaking an investigation.

[4]*The Freedom of Information and Protection of Privacy Act* (hereinafter FOIP), S.S. 1990-91, c. F-22.01.
[5]Email from Ministry A to SK OIPC dated October 19, 2009.
[6]Government of Saskatchewan, *The Career Centre*, accessible at www.careers.gov.sk.ca/.

II ISSUES

1. Does Saskatchewan's *The Freedom of Information and Protection of Privacy Act* prohibit the transfer of personal information outside of Canada?

2. How can the risks of outsourcing be mitigated?

a. Concerns regarding the use of service providers located outside of Canada

b. Legislative changes in Canada in response to concerns of the flow of personal information outside of Canada

c. The role of contracts in mitigating risks

d. Privacy Impact Assessment

III DISCUSSION OF ISSUES

[7] PSC is a government institution for purposes of FOIP.[7] FOIP is engaged as PSC is collecting the personal information of employees and of job applicants.

[8] My authority for this investigation under FOIP is as follows:

> **33** The commissioner may:
> ...
>
> (b) after hearing the head, recommend that a government institution:
>
> (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and
>
> (ii) destroy collections of personal information that is collected in contravention of this Act;

[7] *Supra* note 4 at section 2(1)(d)(i) defines a "government institution" as "the office of Executive Council or **any department**, secretariat or other similar agency **of the executive government of Saskatchewan**". [emphasis added]

> (c) in appropriate circumstances, authorize the collection of personal information in a manner other than directly from the individual to whom it relates;
>
> (d) from time to time, carry out investigations with respect to personal information in the possession or under the control of government institutions to ensure compliance with this Part.[8]

1. Does Saskatchewan's *The Freedom of Information and Protection of Privacy Act* prohibit the transfer of personal information outside of Canada?

[9] In its submission to my office, PSC provided the following reason for choosing Company X as a service provider:

> The [Company X] system was identified by PSC as the best vehicle to collect the employee data as it was readily available, cost effective, user friendly and easily updated to accommodate the collection of data from all employees. In addition, [Company X] had the search and selective access capabilities to make it practicable.
> …
>
> 2. Use of a U.S.A.-based service provider by a government institution in regard to personal information is not prohibited by *The Freedom of Information and Protection of Privacy Act* (FOIP), FOIP does not distinguish between domestic and international transfers of data. Furthermore, Saskatchewan government policy, reflected in the Ministry of Justice and Attorney General's *Personal Information Contract Checklist* does not prevent entering into contracts with U.S.A. based service providers. **As such, it is not illegal nor is it against government policy for government institutions covered by FOIP to enter into contracts with U.S. based companies that require disclosure of personal information. However, government institutions are required to protect personal information**…[9]
>
> [emphasis added]

[10] My office agrees that FOIP does not prohibit using a USA based service provider or contractor. I also agree that government institutions are required to protect personal information in its possession or control in a way that is compliant with FOIP.[10] In other words, government institutions retain their responsibilities under FOIP for the proper

[8] *Ibid.* at section 33.
[9] Letter from PSC to SK OIPC dated February 28, 2012.
[10] I made a similar comment with respect to FOIP in my Investigation Report F-2012-001 at [89], available at www.oipc.sk.ca/Reports/IR%20F-2012-001.pdf.

management of personal information. My office's publication *A Contractor's Guide to Access and Privacy in Saskatchewan*, a resource for contractors of government institutions and local authorities, states as follows:

> The Acts [FOIP and LA FOIP] apply to all records in the possession or under the control of a public body in Saskatchewan. As a contractor or a potential contractor to a public body, you may produce or store records that will be under the control of that public body. These records are subject to the access and privacy provisions of the respective Acts.[11]

[11] The notion that a government institution or local authority, subject to access and privacy legislation, continues to be responsible for records in its control, including in the possession of a contractor, is supported by British Columbia's Office of the Information and Privacy Commissioner (IPC), which stated:

> The fact that outsourcing is contemplated by FOIPPA does not, however, authorize a public body to do so in circumstances that would reduce security arrangements for personal information below those required of the public body directly. **A public body cannot contract out of FOIPPA either directly or by outsourcing its functions. The decision to outsource does not change the public body's responsibilities under FOIPPA. Nor does it change public and individual rights in FOIPPA, which are not balanced against any 'right' to outsource.**[12]
>
> [emphasis added]

[12] Further, Ontario's Information and Privacy Commissioner stated the following about outsourcing:

> The critical question for institutions which have outsourced their operations across provincial or international borders is whether they have taken reasonable steps to protect the privacy and security of the records in their custody and control. **I have always taken the position that you can outsource services, but you cannot outsource accountability.**[13]
>
> [emphasis added]

---

[11] SK OIPC, *A Contractor's Guide to Access and Privacy in Saskatchewan*, available at www.oipc.sk.ca/webdocs/ContractorsGuide.pdf.

[12] Office of the British Columbia Information and Privacy Commissioner, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*, October 2004, at p. 100, available at www.oipc.bc.ca/special-reports/1271.

[13] Ontario Information and Privacy Commissioner, *Privacy Investigation Report PC12-39: Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report*, June 27, 2012 at p. 6, available at www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf.

[13] Since government institutions and local authorities must comply with FOIP and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP)[14] respectively, they must take appropriate steps to manage and safeguard personal information in such a way that they can still meet their duties under FOIP and LA FOIP.

[14] Despite both FOIP and LA FOIP being deficient in not featuring an explicit duty to protect personal information in its possession or control, the Government of Saskatchewan's *Overarching Personal Information Privacy Framework for Executive Government* does require provincial public bodies to protect that personal information.[15] In addition, if the failure to protect results in an unauthorized use or disclosure of the personal information, that would be a breach of FOIP or LA FOIP.

2. How can the risks of outsourcing be mitigated?

a. Concerns regarding the use of service providers located outside of Canada

[15] Below is a compilation of concerns of Privacy Commissioners on the storage of Canadians' personal information in a foreign jurisdiction. The following will provide a brief overview of some of their opinions and how their offices, including my own, have dealt with concerns over Canadians' personal information becoming subject to foreign legislation when it moves outside of Canada.

i. Office of the Saskatchewan Information and Privacy Commissioner

[16] In my office's *2004-2005 Annual Report*, I stated the following regarding the potential risk to the personal information of Saskatchewan residents imposed by the USA PATRIOT Act:

> The FOIP and the LA FOIP Acts both apply to records in the possession or "under the control of a government institution". The consequence is that when personal

[14] *The Local Authority Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. L-27.1.
[15] Government of Saskatchewan, *An Overarching Personal Information Privacy Framework For Executive Government*, September 2, 2003, at p. 18, available at www.gov.sk.ca/news-archive/2003/9/11-648-attachment.pdf.

information is shared with a contractor for a variety of purposes, it will typically continue to be under the control of a department even if it may be in the possession of a private corporation. That personal information continues to be subject to the provisions of the FOIP or LA FOIP Acts.

In November 2004, British Columbia's Information and Privacy Commissioner produced a seminal report on the consequences of the *USA Patriot Act* for public sector organizations in the province of British Columbia. This question arose in that province when it was proposed that the provincial health department might contract out certain health information management work. Questions were raised about the risk that personal health information of British Columbia residents might be vulnerable to disclosure to the FBI and US authorities under anti-terrorism legislation in the United States of America.

Our office was contacted by a number of individuals and organizations that questioned the potential risk to personal information of Saskatchewan residents posed by the *USA Patriot Act*. In response, we have engaged in discussions with our British Columbia counterpart, Mr. David Loukidelis and have carefully reviewed that Commissioner's report. This report is available at www.oipc.bc.ca.

Commissioner Loukidelis has made a number of recommendations for the government of British Columbia and the government of Canada.

A number of those recommendations should be considered by the Legislative Assembly in this province. These include the following:

- Amend the FOIP and the LA FOIP Acts to:

    - Impose direct responsibility on a contractor to a public body to ensure that personal information provided to the contractor by the public body, or collected or generated by the contractor on behalf of the public body, is used and disclosed only in accordance with the FOIP and the LA FOIP Acts.

    - Require a contractor to a public body to notify the public body of any subpoena, warrant, order, demand, or request made by a foreign court of other foreign authority for the disclosure of personal information to which the FOIP or the LA FOIP Acts apply.

    - Require a contractor to a public body to notify the public body of any unauthorized disclosure of personal information under the FOIP or the LA FOIP Acts.

    - Ensure that the Information and Privacy Commissioner has the powers necessary to fully and effectively investigate contractors' compliance with the FOIP and the LA FOIP Acts and to require compliance with the FOIP and the LA FOIP Acts by contractors to public bodies, including powers

to enter contractor premises, obtain and copy records, and order compliance.

- **Make it an offence under the FOIP and the LA FOIP Acts for a public body or a contractor to a public body to use or disclose personal information in contravention of the FOIP and the LA FOIP Acts, punishable by a fine of up to $1 million or a significant term of imprisonment, or both.**

- All public bodies should ensure that they commit, for the duration of all relevant contracts, the financial and other resources necessary to actively and diligently monitor contract performance, punish any breaches, and detect and defend against actual or potential disclosure of personal information to a foreign court or other foreign authority.

- Recognizing that it is not enough to rely on contractors to self-report their breaches, a public body that has entered into an outsourcing contract should create and implement a program of regular, thorough compliance audits. Such audits should be performed by a third party auditor, selected by the public body, that has the necessary expertise to perform the audit and recommend any necessary changes and mitigation measures. Consideration should be given to providing that the contractor must pay for any audit that uncovers material noncompliance with the contract.

In addition, elsewhere in this Annual Report I have discussed the need for an explicit statutory duty to protect personal information such as the provision that exists in the British Columbia FOIP Act.

We canvassed all Saskatchewan departments by forwarding to each deputy minister a short questionnaire to determine the extent of contracting out of personal information. What we requested was the following information:

1. How many current arrangements or contracts does your Department have which permit personal information or personal health information of Saskatchewan residents to be moved, even temporarily, outside of Canada?

2. How many current arrangements or contracts does your Department have which permit personal information or personal health information of Saskatchewan residents to be moved, even temporarily, to another Canadian jurisdiction?

3. Is this an increase or decrease over 2003-2004?

4. What steps has your Department taken to ensure that such personal information or personal health information is not misused once it is outside of Saskatchewan?

Several departments replied directly to our survey. We then received a letter from the Information Technology Office (ITO) of the Saskatchewan government. That office advised that it had gathered this information earlier and "it was decided that the best approach was to have my office respond on behalf of all of executive government (CIC crown corporations are not included in this response)." The ITO response identified 20 different contracting out arrangements involving 11 different departments. Fourteen different contractors are involved. Of these 14 contractors, six are based in the United States and the balance in Canada. Those six contractors account for 11 of the 20 contracting out arrangements.

There have been no changes in security requirements during 2004-2005 for all but four of the contracts. In two of the four we are advised that "new contract language specifically prohibits data from leaving Canada - without prior approval". In another of the four contracts we are advised that the "contract has comprehensive confidentiality requirements" and in the fourth contract, we are advised that "contract states that [the contractor] is compliant with federal privacy act".

We have not had an opportunity to look at the contracts in question but I would make the following observations:

- Compliance with a federal privacy law, either the *Privacy Act* (for public sector organizations) or the PIPEDA (for private sector organizations) provides little comfort. **Saskatchewan residents are entitled to expect that their personal information entrusted to provincial government institutions is subject to the relevant Saskatchewan law, i.e. the FOIP Act and in particular Part IV that deals with privacy.** There are significant differences between these different laws in addition to the fact that the federal government has no mandate to oversee the activities of Saskatchewan government departments. Finally, if personal data is under the control of a Saskatchewan government institution, it is the Saskatchewan privacy law that applies to that data and not a federal privacy law.

- **Contractual provisions addressing confidentiality and security are necessary and important but are, in my view, inadequate in the absence of a specific statutory duty on all public bodies to safeguard personal information reinforced by a statutory offence and substantial penalty. I have addressed elsewhere in this Annual Report the need for amending the FOIP and LA FOIP Acts to include such a duty to safeguard personal information.**

- I want to acknowledge an excellent initiative of Saskatchewan Justice, Saskatchewan Property Management Corporation (SPMC) and the ITO to develop the Personal Information Contract Checklist. I note however that:

    - The Checklist and sample contractual provisions typically ignore access and correction of personal information issues.

- There is a lack of clarity and differentiation between "use" and "disclosure". "Use" refers to what happens with personal information when it is utilized in some fashion by a public body, its agents, employees and contractors. A "disclosure" refers to the movement of personal data from the public sector organization to another organization not under the control of the first organization. In other words, a contractor is in no different position for purposes of the FOIP or LA FOIP Acts than an employee working for a public body.

- There is a need for a brochure or booklet that provides information to contractors. Many smaller businesses, without sophisticated privacy experience and knowledge may be providing contracted services to local authorities such as school divisions or regional health authorities. A Contractor's Guide that could be made widely available to Saskatchewan businesses and non-profit organizations providing fee-for-service for public sector organizations could be modeled on similar publications in many other Canadian provinces.

- There is a need, particularly by smaller provincial bodies, local authorities and health trustees, for a personal information protection schedule that can readily be attached to outsourcing contracts. An excellent model is the model *Privacy Protection Schedule* developed by the British Columbia Ministry of Labour and Citizens' Services, Information Policy and Privacy Branch.

I want to acknowledge the proactive approach taken by the Saskatchewan's Health Quality Council (HQC) to the risk posed by outsourcing. When the HQC was developing its patient feedback survey to assist regional health authorities it considered the risk that existed if personal information was sent to a contractor based in the United States. The HQC decided that it would require modification to the arrangement to ensure that personally identifiable information would not leave Canada.

In conclusion, the USA Patriot Act has served a useful purpose by focusing attention on the risks associated with contracting out information services. I believe however, that the more significant risk is that a contractor may improperly disclose or fail to protect personal information. This can happen within Saskatchewan or beyond and Saskatchewan has not yet installed an adequate protection regime to mitigate that risk.[16]

[emphasis added]

[17] I remain of the view that, in order to address the risk of contracting out information services across the border, legislative amendments to include a duty to protect personal

[16]SK OIPC, *2004-2005 Annual Report*, pp. 26 to 30, available at www.oipc.sk.ca/Reports/AnnualReport04-05.pdf.

information and substantial fines and/or imprisonment for non-compliance with FOIP would be essential to protect personal information that citizens are entrusting to Saskatchewan government institutions. Without that legislative provision, sound contractual language may partially mitigate privacy risks but will not be sufficient to ensure that personal information of Saskatchewan residents is properly managed and safeguarded.

ii. Office of the Privacy Commissioner of Canada

[18] The following is an excerpt from the *Personal Information Protection Electronic Documents Act* (PIPEDA)[17] Case Summary #2005-313 from the Office of the Privacy Commissioner of Canada (OPC). I should note that PIPEDA (referred to as the "Act" in the excerpt below) describes the privacy legislation that applies to private-sector organizations, not public bodies. However, the concern underlying personal information flowing across borders remains the same. Organizations, whether public or private, have obligations under applicable access and privacy legislation in regards to managing personal information.

> The possibility of U.S. authorities accessing Canadians' personal information has been raised frequently since the passage of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001* (*USA PATRIOT Act*). Prior to the passage of this Act, U.S. authorities were able to access records held by U.S.-based firms relating to foreign intelligence gathering in a number of ways.
>
> What has changed with the passage of *USA PATRIOT Act* is that certain U.S. intelligence and police surveillance and information collection tools have been expanded, and procedural hurdles for U.S. law enforcement agencies have been minimized. Under section 215 of the *USA PATRIOT Act*, the Federal Bureau of Investigation (FBI) can access records held in the United States by applying for an order of the Foreign Intelligence Surveillance Act Court. A company subject to a section 215 order cannot reveal that the FBI has sought or obtained information from it.
>
> The risk of personal information being disclosed to government authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, Canadian organizations are subject to similar types of orders to disclose personal

[17] *Personal Information Protection and Electronic Documents Act* (hereinafter PIPEDA) S.C. 2000, c. 5.

information held in Canada to Canadian authorities. Despite the objections of the Office of the Privacy Commissioner, the *Personal Information Protection and Electronic Documents Act* has been amended since the events of September 11th, 2001, so as to permit organizations to collect and use personal information without consent for the purpose of disclosing this information to government institutions, if the information relates to national security, the defence of Canada or the conduct of international affairs.

In addition to these measures, there are longstanding formal bilateral agreements between the U.S. and Canadian government agencies that provide for mutual cooperation and for the exchange of relevant information. These mechanisms are still available.
...

- In the Assistant Commissioner's view, **the real concern underlying these complaints is the prospect of a foreign government accessing Canadians' personal information.**

- She concluded, however, that the Act cannot prevent U.S. authorities from lawfully accessing the personal information of Canadians held by organizations in Canada or in the United States, nor can it force Canadian companies to stop outsourcing to foreign-based service providers. **What the Act does demand is that organizations be transparent about their personal information handling practices and protect customer personal information in the hands of foreign-based third-party service providers to the extent possible by contractual means.** This Office's role is to ensure that organizations meet these requirements. In the case of these complaints, these requirements have been met.[18]

[emphasis added]

iii. Office of the British Columbia Information and Privacy Commissioner

[19] The *Freedom of Information and Protection of Privacy Act* (British Columbia's FOIPPA)[19] in British Columbia has been revised so that public bodies can only store and access the personal information in its custody or control in Canada. Section 30.1 of British Columbia's FOIPPA states as follows:

[18]Office of the Privacy Commissioner of Canada (hereinafter OPC), PIPEDA Case Summary #2005-313, available at www.priv.gc.ca/cf-dc/2005/313_20051019_e.asp.
[19]British Columbia's *Freedom of Information and Protection of Privacy Act* [RSBC 1996] c. 165.

> 30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:
>
> (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;
>
> (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;
>
> (c) if it was disclosed under section 33.1 (1) (i.1).[20]

[20] Around the same time as the above amendment was made to British Columbia's FOIPPA, the then-Information and Privacy Commissioner of British Columbia stated that outsourcing does not change a public body's responsibilities under British Columbia's FOIPPA. He acknowledged, though, that laws applicable in foreign jurisdictions will determine the status and enforceability of the law. He made recommendations that British Columbia's FOIPPA be amended so that service providers notify public bodies if it is ever requested to disclose personal information (that is under the custody or control of the public body). He stated the following in his report *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*:

> Outsourcing is not inconsistent with FOIPPA. It is contemplated by the extended definition of "employee" in Schedule 1 to FOIPPA, which includes "a person retained under contract to perform services for the public body" and, by section 33(f), which permits disclosure to an "employee" of personal information in the custody or under the control of a public body where the disclosure is necessary for the performance of the employee's duties.
>
> The fact that outsourcing is contemplated by FOIPPA does not, however, authorize a public body to do so in circumstances that would reduce security arrangements for personal information below those required of the public body directly. A public body cannot contract out of FOIPPA either directly or by outsourcing its functions. **The decision to outsource does not change the public body's responsibilities under FOIPPA. Nor does it change public and individual rights in FOIPPA, which are not balanced against any 'right' to outsource.**

[20] *Ibid.* amended October 19, 2004 to include section 30.1, available at www.leg.bc.ca/37th5th/3rd_read/gov73-3.htm.

Section 30 requires public bodies to make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information. **When a public body contracts out functions, it must ensure there will be reasonable security arrangements for the personal information that it discloses to the contractor and that the contractor collects or generates in fulfilling the outsourced function.** The public body's responsibilities under section 30, and the required standard of security, are constants, with or without outsourcing.

Submissions to us from the BC government and from contractors alike agree that, when a contractor possesses personal information in connection with outsourcing of public body functions, the personal information continues to be under the public body's control under FOIPPA. **They emphasize that their diligence in this respect includes fashioning contract terms that embody FOIPPA obligations, thereby ensuring that the personal information "enjoys substantially the same protection it enjoyed prior to being made available to an outsourcing partner".** The public body is bound to comply with FOIPPA and the contractor is contractually bound not to disclose information without the authority of the public body.

Ongoing public body control of personal information under FOIPPA and the contractual extension of public body FOIPPA obligations to contractors do not resolve concerns about data that is sent abroad to places where FOIPPA is not the law and is neither respected nor enforced by the legal system abroad. Without a nation-to-nation accord that provides otherwise, data that travels to the US is subject to US law, including FISA. A British Columbia public body could try to live up to its FOIPPA responsibilities through its contract with a US-located contractor, but US law would all but inevitably determine the status and enforceability in the US of those contract terms.

The British Columbia government said in its submission to us that it would address this situation by committing not to send sensitive personal information to the US either on a temporary or permanent basis. This is constructive. It raises the question of whether this commitment will also apply for public bodies under FOIPPA that are not part of a government ministry. We believe there is no reason in principle, if such a commitment is implemented, not to extend it further. Indeed, the need for protection of personal information of British Columbians held by public bodies under FOIPPA is as compelling for Schedule 2 and 3 public bodies as it is for ministries of the provincial government. Many Schedule 2 public bodies—such as hospitals and other health care bodies—hold extremely sensitive personal information about patients. Many Schedule 3 public bodies—such as self-governing professional and occupational bodies—hold extremely sensitive personal information about their members and about their members' clients or patients. **It also raises the question of whether FOIPPA should be amended to make this commitment a statutory requirement. We think this should be seriously explored by the British Columbia government.**

The British Columbia government also says it intends to amend FOIPPA to "expressly prohibit service providers from disclosing personal information that

> **has been provided to them by public bodies unless permitted by [FOIPPA], and require that such service providers notify government in the event their foreign affiliate requests that they disclose such information". These would be important new safeguards for personal information that contractors hold in British Columbia under outsourcing arrangements with public bodies, whether or not the contractors have corporate or other links to the US.**[21]
>
> [emphasis added]

[21] Further, in my office's *2005-2006 Annual Report*, I noted how the former Saskatchewan Information and Privacy Commissioner, Richard Rendek, made a recommendation to Saskatchewan government institutions to adapt the recommendations of the then Information and Privacy Commissioner of British Columbia. Further, and as mentioned earlier in this Investigation Report, I recommended that Saskatchewan Justice follow the British Columbia government in their development of its *Privacy Protection Schedule*[22]. I stated:

> I note that the last Commissioner, Richard Rendek, recommended to government institutions in early 2003 that the recommendations from the British Columbia Information and Privacy Commissioner on outsourcing personal information be adapted for Saskatchewan. Subsequently, the British Columbia government developed a standard *Privacy Protection Schedule*. I find that this is a relatively simple, efficient and accurate way of addressing through contract the privacy risks inherent with outsourcing personal information. In considering the approach taken in other Canadian jurisdictions, it appears that the British Columbia model is consistent with privacy 'best practices'. A number of the Crown corporations have adapted that British Columbia model for use in their outsourcing contracts. I recommend that Saskatchewan Justice follow that approach so that we can minimize confusion and ensure government institutions meet privacy best practices in their contracting out activities.[23]

[22] I have not advocated for legislative amendments to prohibit the outsourcing of information services beyond the provincial or Canadian borders. However, I have advocated for legislative amendments to FOIP and LA FOIP including a 'duty to protect' provision that imposes the duty on government institutions and local authorities to

---

[21] *Supra* note 12 at pp. 100 to 101.
[22] British Columbia Government, *Privacy Protection Schedule*, available at www.cio.gov.bc.ca/cio/priv_leg/foippa/contracting/ppsindex.page.
[23] SK OIPC, *2005-2006 Annual Report*, at pp. 18 to 19, available at www.oipc.sk.ca/Reports/AnnualReport05-06.pdf.

safeguard personal information in its possession or control. Further, I have encouraged government institutions and local authorities to have provisions in their contracts with service providers to ensure that privacy 'best practices' are reflected such as those modeled by British Columbia Government's *Privacy Protection Schedule*.

iv. Office of the Alberta Information and Privacy Commissioner

[23] The Alberta IPC issued a report called *Public-Sector Outsourcing and Risks to Privacy* in February 2006 and stated the following in regards to risks from public-sector outsourcing:

> **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.[24]

[emphasis added]

[24] Also in the above report, the Alberta IPC included a list of topics a public body's contract should include when outsourcing to a third-party:

> 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

[24]Office of the Alberta Information and Privacy Commissioner (AB IPC), *Public-sector Outsourcing and Risks to Privacy*, February 2006, at pp. 9 to 10, available at www.oipc.ab.ca/Content_Files/Files/Publications/Outsource_Feb_2006_corr.pdf.

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:

…

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.[25]

[25] This concludes my summary of concerns over the storage of Canadians' personal information in foreign jurisdictions identified by my office and by several Information and Privacy Commissioners from across Canada. Next, I will review legislative changes in different Canadian jurisdictions that have been made to address such concerns.

b. Legislative changes in Canada in response to concerns of the flow of personal information outside of Canada

[25] *Ibid.* at pp. 33 to 34.

[26] The concern surrounding the flow of personal information outside of Canada is exemplified by the legislative changes in several Canadian jurisdictions.

[27] As mentioned earlier, British Columbia has amended its FOIPPA to state that public bodies can only store and access personal information within Canada.

[28] Nova Scotia has introduced legislation called the *Personal Information International Disclosure Protection Act* (Nova Scotia's PIIDPA)[26] that states that public bodies can only store and access personal information in Canada. However, Nova Scotia's PIIDPA also outlines limited circumstances in which public bodies may disclose personal information outside of Canada.[27]

[29] In 2006, Alberta IPC provided recommendations for legislative changes to Alberta's *Freedom of Information and Protection of Privacy Act* (Alberta's FOIP)[28] in its document *Public-sector Outsourcing and Risks to Privacy*, including amending section 40(1)(g):

> Amend section 40(1)(g) of the *Freedom of Information and Protection of Privacy Act* and section 35(1)(i) of the *Health Information Act* to make it clear that personal information can only be disclosed pursuant to an order of a Canadian court having jurisdiction. [29]

[30] Section 40(1)(g) of Alberta's FOIP was amended by the Alberta government to read as follows:

> 40(1) A public body may disclose personal information only
>
> ...
>
> (g) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information,[30]

[26]Nova Scotia's *Personal Information International Disclosure Protection Act*, Chapter 3 of the Acts of 2006.
[27]*Ibid*. at section 5.
[28]Alberta's *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25.
[29]*Supra* note 24 at p. 33.
[30]*Supra* note 28 at section 40(1)(g).

[31] The Alberta Government explained in its publication *FOIP Bulletin No. 18* as follows:

> Section 40(1)(g) has been amended to state that a public body may disclose personal information for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction *in Alberta* to compel the production of information or with a rule of court *binding in Alberta* that relates to the production of information. (The italicized words have been added).
>
> This amendment makes it clear that a public body, and anyone acting on its behalf, may disclose personal information in response to a subpoena, warrant or order of a court or tribunal, or to comply with a court rule, *only* if the court or tribunal has the power in Alberta to require the public body to disclose the information.
> ...
>
> This amendment addresses situations where a contractor providing services for or on behalf of a public body holds personal information relating to the services and a foreign court issues an order for production of that information. This situation may arise where
>
> - the information is in or accessible from a foreign location,
> - the contractor is subject to the laws of the foreign jurisdiction, or
> - the contractor is affiliated with an organization that is subject to the laws of the foreign jurisdiction.
>
> Whether or not the order relating to the information is binding on the contractor will depend on the rules relating to conflict of laws.
>
> The FOIP Act has also been amended to establish offence and penalty provisions for disclosure in response to a subpoena, warrant or order if
>
> - the disclosure is not permitted under section 40(1)(g), and
> - no other provision of the FOIP Act permits disclosure.
>
> …
>
> The impetus for this amendment was United States legislation (the *USA PATRIOT Act*) which expanded the powers of U.S. law enforcement to obtain orders from the Foreign Intelligence Surveillance Court. This Court can issue orders that require a person to produce information in secrecy.
>
> **However, the FOIP Act amendment has broader application. In any context where personal information crosses jurisdictional boundaries, or where the laws of another jurisdiction apply to a public body's contractor, there is the possibility that a court in that other jurisdiction will order disclosure of personal information. Section 40(1)(g) makes it clear that a public body, which is**

> **responsible for compliance with the FOIP Act, must not allow unauthorized disclosure in response to this kind of court action.**[31]
>
> [emphasis added]

[32] Alberta also amended its private-sector legislation, *Personal Information Protection Act* (Alberta's PIPA)[32] so that private sector organizations must provide notification to individuals if their personal information will be collected by a service provider outside of Canada for or on behalf of the organization, or if personal information will be transferred to a service provider outside of Canada:

> **13.1(1)** Subject to the regulations, an organization that uses a service provider outside Canada to collect personal information about an individual for or on behalf of the organization with the consent of the individual must notify the individual in accordance with subsection (3).
>
> **(2)** Subject to the regulations, an organization that, directly or indirectly, transfers to a service provider outside Canada personal information about an individual that was collected with the individual's consent must notify the individual in accordance with subsection (3).
>
> **(3)** An organization referred to in subsection (1) or (2) must, before or at the time of collecting or transferring the information, notify the individual in writing or orally of
>
> (a) the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and
>
> (b) the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization.
>
> **(4)** The notice required under this section is in addition to any notice required under section 13.[33]

[33] Further, there have been recommendations made by Information and Privacy Commissioners from across Canada, including me, to governments to amend applicable

[31] Government of Alberta, Service Alberta, *FOIP Bulletin No. 18*, at pp. 6 to 8, available at www.servicealberta.ca/foip/documents/bulletin18.pdf.
[32] Alberta's *Personal Information Protection Act*, S.A. 2003, c. P-6.5.
[33] *Ibid.* at section 13.1.

access and privacy legislation to address concerns surrounding the outsourcing of personal information outside of Canada.[34] I have stated since 2003 that a 'duty to protect' provision should be included in FOIP and LA FOIP.[35] Such a provision helps address the increased risk associated with modern challenges such as the USA PATRIOT Act.[36]

[34] It is beyond the ability of PSC to make legislative changes to FOIP to address the risks associated with the transferring of personal information beyond Canada's borders. However, I would like to address the topic briefly because my office has a mandate to provide advice to the Legislative Assembly of Saskatchewan as well as public bodies.

[35] As mentioned earlier, a few jurisdictions in Canada have made amendments or introduced legislation to manage the risk of outsourcing. In my office's February 2006 edition of the *Saskatchewan FOIP FOLIO*, my office stated the following in regards to the deficiency in our province's FOIP in addressing risks associated with outsourcing:

> As noted in our Annual Report 2004-2005, our Saskatchewan FOIP Act is deficient in not imposing any duty on public bodies to protect personal information in their possession or under their control. There is therefore no offence to fail to protect personal information in the control of a public body. If however an improper disclosure to someone results from the failure to protect, there is a violation of the Act. There is no substantial penalty to underscore the importance of this responsibility. Fines under more recent privacy laws are very substantial ($500,000 in HIPA, $100,000 in PIPEDA, B.C.) The maximum fine under our Saskatchewan FOIP Act is $1,000.
>
> The Saskatchewan government has suggested some changes to its outsourcing contracts but is apparently not planning to address these risks through legislative change.[37]

[36] Our province's Provincial Auditor has also recommended that the government consider legislative changes to address risks associated with the USA PATRIOT Act as follows:

---

[34] *Supra* note 24 at p. 33; OPC, *Annual Report to Parliament 2004-2005: Report on the Privacy Act*, at pp. 19 to 20, available at www.priv.gc.ca/information/ar/200405/200405_pa_e.pdf.
[35] SK OIPC, *2003-2004 Annual Report*, at p. 21, available at www.oipc.sk.ca/Reports/AnnualReport03-04.pdf; *Supra* note 16 at pp. 14 to 15.
[36] *Supra* note 23 at p. 11.
[37] SK OIPC, February 2006 *Saskatchewan FOIP FOLIO*, available at www.oipc.sk.ca/FOIPFOLIO/February2006.pdf.

> One further way to protect data is through legislation. We have consulted with Saskatchewan's Information and Privacy Commissioner regarding PAC's [Public Accounts Committee's] request and this study. The Commissioner has identified that Saskatchewan's legislation is out of date, observing that "all other provinces in western Canada and most Canadian jurisdictions have extensively revised and modernized their access and privacy laws."
> In particular, the Commissioner has noted that more recent laws in Canada include a "duty to protect" that requires government agencies to protect personal information. This duty is backed up by significant penalties. Such protections, which are present in Saskatchewan's [sic] *Health Information Protection Act*, are absent in Saskatchewan's general access and privacy legislation.
>
> **The Commissioner has recommended that the legislation be amended. According to the Commissioner, adequate legislative protection would reinforce the need for government agencies to ensure they have carefully assessed risks and have been diligent in using contracts to manage the risks. We agree. In addition, we also agree with the Commissioner that legislative responses to the USA Patriot Act in other provinces should be carefully considered for Saskatchewan.**
>
> 1. We recommend that the Ministry of Justice and Attorney General consider the benefits, in consultation with Saskatchewan's Information and Privacy Commissioner, of changes to Saskatchewan's general access and privacy legislation, which could serve to mitigate risks related to the USA Patriot Act. In particular, Saskatchewan's Information and Privacy Commissioner has expressed concerns and made recommendations regarding the "duty to protect" personal information and data in prior years.[38]
>
> [emphasis added]

[37] In spite of the above, the Saskatchewan government has not amended either FOIP or LA FOIP to better protect Saskatchewan residents' personal information, nor has it even indicated it is prepared to do so.

[38] However, I was advised on February 5, 2013 by the Saskatchewan Government that it is undertaking a review of "privacy-related" legislation:

> Currently the government is undertaking a review of privacy-related legislation. In light of that review, and without prejudging the outcome of that review, we feel that it

[38]Provincial Auditor of Saskatchewan, *2011 Report – Volume 2*, at pp. 410 to 411, available at www.auditor.sk.ca/wp-content/uploads/2012/05/20_Protecting-Sask-data.pdf.

> would be more appropriate to make a decision with regard to additional financial or personnel resources in that office once that review has been concluded.[39]

[39] I recommend that in its review, the Government of Saskatchewan amend FOIP and LA FOIP to include an explicit duty upon public bodies to protect personal information in its possession or control. I further recommend that the failure to protect that personal information is made an offence and exposes the offending public body to a large fine.

c. The role of contracts in mitigating risks

[40] Contracts are a tool that can help mitigate the risk of outsourcing services to contractors. Saskatchewan Justice Access and Privacy Branch's *Personal Information Contract Checklist Version 2.2* (Checklist) states the following in regards to contracts:

> In 2003, the Government of Saskatchewan approved *An Overarching Personal Information Privacy Framework for Executive Government* which, among other things, **directed that government organizations take steps in all outsourcing contracts to protect personal information.** This resulted in the creation of a Personal Information Contract Checklist, which was circulated to all government organizations in 2004.[40]
>
> [emphasis added]

[41] Further, the Government of Alberta's *Managing Contracts under the FOIP Act* states the following in regards to the importance of contracts in ensuring compliance with Alberta's FOIP:

> …it is important to establish the obligations of the contractor within the contract for several reasons.
>
> First, a public body is legally responsible for the compliance of its contractors with the requirements of the Act and the contract is a means of ensuring compliance.
> Second, the FOIP Act is an Act of general application; it sets out a number of general principles that apply to a very broad range of programs and services. The contract

[39]Legislative Assembly of Saskatchewan, Board of Internal Economy, *Hansard Verbatim Report*, February 5, 2013, at p. 39, available at http://docs.legassembly.sk.ca/legdocs/Legislative%20Committees/BIE/Hansard/130205Debates-BIE.pdf.
[40]Saskatchewan Justice Access and Privacy Branch, *Personal Information Contract Checklist, Version 2.2*, May 2007 at p. 2, available at www.justice.gov.sk.ca/PICC.

> allows the public body to provide clarity with respect to its understanding of how the Act applies within the specific circumstances of the matter to be governed by the contract.
>
> Third, the contract allows public bodies to specify adherence to policies and best practices that may not be required under the Act but have been adopted as standard for government operations.
>
> Finally, the contracting process provides an opportunity to address matters that are not addressed in the FOIP Act, but which are necessary to ensure effective management of matters relating to the contractor's obligations, such as the monitoring of performance.[41]

[42] Below, I will review provisions within the contract between PSC and Company X and how they address the risk when outsourcing services.[42]

i. Amendments to the PSC contract with Company X in 2010

[43] The contract between PSC and Company X was originally signed in 2002. It was renewed in 2006. It was renewed again in 2010 but amendments were made to the contract to address privacy issues. Section 9 of the original contract in 2002 stated:

> **9 CONFIDENTIAL INFORMATION**
>
> 9.1 Definition of Confidential Information
>
> For the purposes of this Agreement, "Confidential Information" means any and all (i) technical and non-technical information including patent, trade secret and proprietary information, techniques, sketches, drawings, models, inventions, know-how, processes, apparatus, equipment and algorithms related to the Application, the Site, the Platform, [Company X] Content, and related documentation, (ii) information relating to costs, prices and names, finances, marketing plans, business opportunities, personnel, research, development or know-how; (iii) all non-public Province Data; and (iv) information designated by either party as confidential in writing or, if disclosed orally, designated as confidential at disclosure and reduced to writing and provided to the other party within thirty (30) days of disclosure. Notwithstanding the foregoing,

[41]Government of Alberta, *Managing Contracts under the FOIP Act*, at p. 63, available at www.servicealberta.ca/foip/documents/contractmanager.pdf.

[42]For guidance in contract elements, public bodies should also refer to my Investigation Report H-2011-001 at [200] to [201] where I provide a list what Saskatchewan trustees should consider including in any contract with an information management service provider, available at www.oipc.sk.ca/Reports/IR%20H-2011-001.pdf.

> "Confidential Information" shall not include information that: (1) is or becomes generally known or available by publication, commercial use or otherwise through no fault of the disclosing party; (2) is known and has been reduced to tangible form by the disclosing party at the time of disclosure and is not subject to restriction; (3) is independently developed or learned by either party; (4) is lawfully obtained from a third party who has the right to make such disclosure; or (5) is released for publication in writing.
>
> [Company X] understands and is aware that all invoices and expenses associated with this project may be required to be disclosed through the Rules of the Legislative Assembly of Saskatchewan Public Accounts and/or the audit process as per the Financial Administration Act, 1993.[43] Any such disclosure shall not be considered a breach or violation of this Section 9.1.
>
> 9.2 Nondisclosure and Nonuse Obligation
>
> Each party agrees that it will not and will ensure that its employees, agents and contractors will not make use of, disseminate, or in any way disclose any Confidential Information of the other party to any person, firm or business, except for any purpose the disclosing party may hereafter authorize in writing. Each party agrees that it will treat all Confidential Information with the same degree of care as it accords to its own Confidential Information, and each party represents that it exercises reasonable care to protect its own Confidential Information.[44]

[44] PSC, also, provided my office with a copy of its *Amending Agreement No. 1* that amended Section 9 of the Agreement in 2010 as follows:

> 3. Section 9 of the Agreement is amended as follows:
>
> (a) The second paragraph of Section 9.1 is amended by replacing the words "[Company X] understands and is aware that all invoices and expenses associated with this project may be required to be disclosed through the Rules of the Legislative Assembly of Saskatchewan Public Accounts and/or the audit process as per the Financial Administration Act, 1993. Any such disclosure shall not be considered a breach or violation of this Section 9.1" with "[Company X] understands and is aware that this agreement, and invoices and expenses associated with this Agreement may be disclosed publicly as a result of the Province's execution process, through the Rules of the Legislative Assembly of

[43]It is curious that the obligations under *The Financial Administration Act, 1993* are explicitly preserved but there is no parallel treatment of Parts II and III of FOIP which is made paramount by version of section 23.

[44]Contract between PSC and Company X, signed and dated February 20, 2002 by the Chair of the PSC. Remarkably, although FOIP would have been in force for a decade before the original contract, the protection of personal information is not even identified as an element of "confidential information" in article 9 of that 2002 contract.

Saskatchewan or Public Accounts. Any such disclosure shall not be considered a breach or violation of this section 9."

(b) Section 9.2 is replaced by the following:

9.2 Each party agrees that it will:

(a) protect and secure the Confidential Information of the other party to ensure that it remains confidential and will not disclose the same to any third party without the express written authorization of the other party;

(b) not use the Confidential Information for any purpose other than for the provision of Services under this Agreement. In that regard [Company X] agrees that it will:

(i) keep Province Data logically separate and apart from other customers information and will not combine the information with any other customers information; and

(ii) only divulge Province Data to those of its officers and employees who require such for the performance of this Agreement and will ensure such officers and employees are aware of and comply with the provisions of this section 9;

(c) immediately report to the other where one party knows of or suspect that:

(i) there has been a breach of the party's obligations under section 9, or

(ii) that the confidentiality of the Confidential Information of the other party has been compromised;

(d) promptly return the Confidential Information to the other party, or destroy the Confidential Information in a manner reasonably approved by the other party and provide written confirmation that it has been so destroyed, when it is no longer required to provide Services, and in any event no later than 30 days after the termination or expiration of this Agreement.

9.3 If to provide the Services [Company X] must disclose or make accessible any Province Data to a third party, before doing so [Company X] will obtain from the third party a written agreement under which the third party agrees to be bound by confidentiality obligations at least as restrictive as those contained in this section 9 applicable to [Company X].

9.4 Nothing in this section prevents either party from disclosing any Confidential Information which is necessary to comply with any applicable statute or other law requiring such disclosure, providing where possible, notice is given to the other

party prior to such disclosure being made to permit the other party to object or obtain a court order to prevent such disclosure.

9.5 This section shall survive the expiration or termination of this Agreement.

4. The Following [sic] is added after section 9:

9A CRIMINAL RECORD CHECKS

9A.1 [Company X] shall not, without the prior written approval of the Province, assign anyone to provide services under this Agreement whom [Company X] knows to have a criminal record.

9A.2 [Company X] shall ensure that:

a) a criminal record check ("CRC") has been performed on anyone employed by [Company X] to provide services under this Agreement

On the request of the Province, [Company X] will provide written verification that the CRC of any particular employee providing services under this Agreement discloses no criminal record.

9A.3 At the Province's cost, the Province may reasonably request any one employed by [Company X] to provide services directly to the Province under this Agreement to undergo a new CRC where the Province has objective and quantifiable information to suggest the employee may have recently obtained a criminal record.[45]

[45] Section 9 and its amendments certainly enhance the privacy protections of the information being stored, including requiring Company X to notify PSC when: 1) a request is received by Company X to disclose the personal information to a third party, and 2) when the confidence of "Confidential Information" has been breached. Further, the amendment states that Company X's employees will only access the information on a "need-to-know" basis to fulfill the purposes of the contract, and that information will be returned to PSC or destroyed at the end of termination or expiration of the contract.

[46] It is clear, as PSC has pointed out to us, that it referred to the Saskatchewan Justice's Checklist when making such amendments to the contract. The Checklist includes the following recommendations:

[45] *Amending Agreement No. 1* between Company X and PSC dated March 4, 2010.

The contract should require the Contractor to:

- keep the information provided in confidence and not further disclose it, unless the services require it.
- not use the information for any purpose other than providing the services
- report to you immediately if there is any suspicion the information has been compromised, or when an order, warrant or any other document purporting to compel production of the information has been served upon the Contractor.
- permit you to audit the Contractor's security practices.
- return the information to you or to destroy the information when the contract has expired or is terminated. You may want to consider if any part of the information should be destroyed more frequently (for example, in a long term contract for mailing out information, should the information be destroyed shortly after each mail out?)
- where the contract requires subcontractor services, that the subcontractor be approved by the department and sign a commitment in favour of the department or institution to protect the information to the same degree as the Contractor[46]

[47] Despite the amendments to the 2002 contract, there are still a number of things missing. Below are recommendations for further amendments to the contract to address privacy issues.[47] The information collected, used or disclosed pursuant to the contract is subject to the provisions of FOIP and *The Health Information Protection Act* (HIPA)[48] (where applicable).

a. Definitions

[48] FOIP applies to records and recorded personal information in the possession or control of a government institution. Therefore, the definition of "personal information" as defined by section 24 of FOIP respectively should be included in the contract.

[46] *Supra* note 40.
[47] References drawn from *Supra* note 41.
[48] *The Health Information Protection Act*, S.S. 1999, c. H-0.021.

[49] Unfortunately, the contract between PSC and Company X does not define "personal information". It defines "Province Data" as follows:

> 1.6 "Province Data" means any and all information (including without limitation, Candidates information and job postings data and otherwise) provided, inputted or uploaded to the Application by an Authorized User or Applicant.[49]

[50] Further, as stated in the body of the analysis, the contract also defines "Confidential Information" as:

> "Confidential Information" means any and all (i) technical and non-technical information including patent, trade secret and proprietary information, techniques, sketches, drawings, models, inventions, know-how, processes, apparatus, equipment and algorithms related to the Application, the site, the Platform, [Company X] Content, and related documentation, (ii) information relating to costs, prices and names, finances, marketing plans, business opportunities, personnel, research, development or know-how; (iii) all non-public Province Data; and (iv) information designated by either party as confidential in writing or, if disclosed orally, designated as confidential at disclosure and reduced to writing and provided to the other party within thirty (30) days of disclosure. Notwithstanding the foregoing, "Confidential Information" shall not include information that: (1) is or becomes generally known or available by publication, commercial use or otherwise through no fault of the disclosing party; (2) is known and has been reduced to tangible form by the disclosing party at the time of disclosure and is not subject to restriction; (3) is independently developed or learned by either party; (4) is lawfully obtained from a third party who has the right to make such disclosure; or (5) is released for publication in writing.[50]

[51] I find the above dense and confusing, and certainly fails to highlight the obligation to protect personal information.

[52] Personal information is different from other types of information. FOIP recognizes such a distinction since Part IV of FOIP speaks specifically as to how personal information should be managed. Therefore, personal information should not be lumped together or treated like all other types of information. The failure to distinguish personal information from other types of information is a hindrance in ensuring contractors comply with FOIP obligations under Part IV of FOIP.

[49] *Supra* note 44.
[50] *Ibid.*

[53] In my office's *2005-2006 Annual Report*, I stated the following in regards to the lack of guidance in the Checklist to government institutions including the need for definitions of "personal information" and "personal health information" in contracts:

> Saskatchewan Justice has also produced a number of sample clauses. **The sample clauses that we have seen characterize all information provided by a government institution to a contractor as "confidential information". This is problematic since the issues in terms of 'proprietary information' of any government institution are different than the privacy interests of Saskatchewan residents. Conflating personal information/personal health information with other kinds of information fails to adequately address the very real threats to privacy posed in 2006.** Public sector employees should be clear that personal information of individuals needs to be identified, collected, used and disclosed only in accordance with FOIP, LA FOIP and privacy best practices such as a 'need to know' requirement and the requirement to use aggregate information or de-identified information wherever possible and to use personal information only when aggregate information or de-identified information would not be sufficient for the purpose.
>
> At the same time, these sample clauses are problematic in terms of the transparency obligations of government institutions under Part II of FOIP. **Describing all information provided by government to the contractor as confidential is inconsistent with the requirements of FOIP.** There is no exemption for "confidentiality" generally and the government institution is required to consider and invoke only the mandatory or discretionary exemptions detailed in FOIP. Contractors may be encouraged by the standard contract language to assume that all or most of the information involved in any contract with government will not be accessible under FOIP. This approach will likely be misleading to contractors and government workers alike. **Rather, contracts should use the definition of "personal information" from section 24 of FOIP.**[51]
>
> [emphasis added]

[54] In my office's letter dated November 15, 2012 to PSC, my office recommended that the definition of "personal information" from FOIP be included in the contract.

[55] In its letter dated March 22, 2013, PSC provided my office with the following language that would be included in its contract with Company X:

> **2: "Personal Data"** means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one

[51] *Supra* note 23 at p. 18.

> or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.
>
> **3 "Categories of Personal Data":** Personal Data may include, among others, personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, social security details and business contact details; financial details; and goods and services provided.
> …
>
> **1. Agreement Definitions**
>
> **1.18. "Your Content"** means all text, files, images, graphics, illustrations, information, data (including Personal Data as that term is defined in the Data Processing Agreement for [Company X] Cloud Services), audio, video, photographs and other content and material (other than Your Applications), in any format, provided by You or Your Users that reside in, or run on or through, the Services Environment.

[56] The above contract language does better to capture the definition of "personal information" as stated in FOIP. However, PSC did not provide my office with an explanation as to why it did not simply use the definition of personal information from FOIP.

b. Records Management

[57] Since the contractor would be maintaining personal information on behalf of the government institution, the contract should specify the nature of the information in question and the contractor's obligations with respect to same. Below is a discussion about the provisions in the contract that relate to topics such as possession or control, and retention and disposition:

i. Possession or Control

[58] In my Review Report LA-2010-002, I discussed possession and control:

[35] I discussed the issue of possession and control in my Report F-2008-002 as follows:

> [23] In *Canada Post Corp. v. Canada (Minister of Public Works)*, the minority opinion included the following helpful comments regarding the difference between possession and control:
>
> > 28… in their normal and proper sense, the two words "control" and "possession" do not signify the same concept. **"Control" connotes authority whereas "possession" merely indicates custody.** It is true that they are used interchangeably in some contexts, but that occurs because normally one is an attribute of the other. Possession is usually a consequence of control. To say … that a person who has possession of a thing has some control over it simply means that a person has one of the basic attributes of control. There is no such thing as a proportion of control. While I am prepared to agree with the motions judge that the dictionary definition alone cannot solve the problem, it is necessary to recognize that, in common but proper language, "control" and "possession" do not have the same meaning and cannot be taken one for the other.
> >
> > …
>
> [25] In order for a record to be subject to an access to information request, the public body need only have possession or control, not both. This is demonstrated through the legislature's choice to join the two terms with 'or', rather than 'and'.
> ...
>
> [51] I have attempted, when permitted by LA FOIP, to interpret and apply its provisions in a manner that is largely consistent with other Canadian oversight agencies. **That approach in this case requires a consideration of 'control' as a factor assessing whether there is possession** and whether LA FOIP applies to the record in question.[52]
>
> [emphasis added]

[59] FOIP dictates how government institutions are to provide access to records as well as how it ought to manage personal information. Contracts are a means for a government institution to maintain control of records when working with a contractor so that it can ensure it is in compliance with FOIP. For example, sections 5 and 31(1) of FOIP provides individuals with a right to access records and personal information in the possession or control of a government institution. Section 5 of FOIP provides as follows:

[52]SK OIPC, Review Report LA-2010-002, available at www.oipc.sk.ca/review.htm.

> **5** Subject to this Act and the regulations, every person has a right to and, on an application made in accordance with this Part, shall be permitted access to records that are **in the possession or under the control** of a government institution.[53]
>
> [emphasis added]

[60] Further, section 31(1) of FOIP provides as follows:

> **31**(1) Subject to Part III and subsection (2), an individual whose personal information is contained in a record **in the possession or under the control** of a government institution has a right to, and:
>
> (a) on an application made in accordance with Part II; and
>
> (b) on giving sufficient proof of his or her identity;
>
> shall be given access to the record.[54]
>
> [emphasis added]

[61] In order for government institutions to comply with FOIP, it must stipulate in contracts that it maintains control over the records related to the contract that may be in the possession of the contractor.

[62] In Order F2010-023 of the Alberta IPC, a contractor of the public body (which is subject to Alberta's FOIP) refused to provide the public body access to records that were responsive to an access to information request. However, the adjudicator found that the public body maintained control over records that were in the possession of a contractor because the contract between the public body and contractor stipulated that the records were the "absolute property" of the public body. Therefore, the adjudicator ordered the public body to retrieve the records from the contractor in order to respond to the access to information request.[55]

[53] *Supra* note 4 at section 5.
[54] *Ibid.* at section 31(1).
[55] AB IPC, Order F2010-023 at para 68, 100 and 101, available at www.oipc.ab.ca/downloads/documentloader.ashx?id=2785.

[63] Further, in the Order MO-2770 by the Ontario IPC, the adjudicator found that the public body in that case (which is subject to Ontario's *Municipal Freedom of Information and Protection of Privacy Act*[56]) had control of records that were in the possession of the contractor. An access to information request was submitted to the public body but the public body stated it did not have possession or control over the records. However, the adjudicator who reviewed the agreement between the public body and contractor stated that the public body had "'full and free access' to records that are 'pertinent to the operations under the terms of the agreement.'"[57] Therefore, the adjudicator found that the public body indeed had "control" of the records in the possession of the contractor in that case.

[64] Section 5.2 of the contract between PSC and Company X states as follows:

> 5.2 Province Rights
>
> All right, title and interest in and to the Province Data and Deliverables shall remain exclusively with Province and its licensors, as applicable. Except as set forth in Section 2.1(f) or Section 9, without the permission of Province, access to the Province Data is provided to [Company X] only to allow [Company X] to fulfill its obligations under this Agreement, including without limitation to diagnose and provide services at Province's request in relation to the site and Platform.[58]

[65] The above contract provision states that Company X may only use information in accordance with the Agreement but that PSC maintains "all rights" to the information. My office made the recommendation in its letter dated November 15, 2011 that the provision needs to be stronger by stating that PSC may access the information in the possession of Company X so that PSC can comply with its obligations under FOIP, including the search for responsive records in response to access to information requests.

[66] PSC in its letter dated March 22, 2013 provided my office with the following language to be included in the newly-negotiated contract with Company X:

[56]Ontario's, *Municipal Freedom of Information and Protection of Privacy Act* R.S.O. 1990, c. M.56.
[57]Office of the Ontario Information and Privacy Commissioner, Order MO-2770 at [40], available at www.ipc.on.ca/images/Findings/MO-2770.pdf.
[58]*Supra* note 44.

> **5. Owner of Data**
> The ownership and control of Personal Data remains with Customer, and Customer will at all times remain the Data Controller. Customer is responsible for compliance with its obligations as data controller under data protection laws, in particular for justification of any transmission of Personal Data to [Company X] (including providing any required notices and obtaining any required consents), and for its decision concerning the processing and use of the data.
>
> **6. Rights of Data Subject**
> [Company X] will grant Customer electronic access to Customer's subscribed Cloud Services Environments that hold Personal Data to permit customer to delete, release, correct or block access to specific Personal Data or, if that is not practicable and to the extent permitted by applicable law, follow Customer's detailed written instructions to delete, release, correct or block access to Personal Data. Customer agrees to pay [Company X's] reasonable fees associated with the performance of any such deletion, release, correction or blocking of access to data. [Company X] shall pass on to the Customer contacts identified in Section 15 below any requests of an individual to delete, release, correct or block Personal Data processed under the Agreement.

[67] The above provisions address my office's recommendations that the contract clearly states that PSC retains control over the information and that Company X must locate and retrieve information stored by it, upon request by PSC.

ii. Retention and Disposition

[68] Each government institution should have its own retention and disposition schedule that apply to the records being maintained by the contractor on behalf of the government institution. Such retention and disposition schedules should be included as part of the contract. The contract should stipulate whether the records are to be transferred back to the government institution at the end of the retention period for destruction or the contractor is to destroy the records on behalf of the government institution. The contract should also state how the records are to be destroyed, including notification being provided to the government institution prior to destruction.[59]

[59] *Supra* note 42 at [201] to [203], I discuss elements that should be included in a contract between a Saskatchewan trustee and an information management service provider.

[69] Section 9.2(d) of *Amending Agreement No. 1* between PSC and Company X addresses the destruction of records:

> 9.2 Each party agrees that it will:
> …
>
> (d) promptly return the Confidential Information to the other party, or destroy the Confidential Information in a manner reasonably approved by the other party and provide written confirmation that it has been so destroyed, **when it is no longer required to provide Services, and in any event no later than 30 days after the termination or expiration of this Agreement.**[60]
>
> [emphasis added]

[70] The language is very vague when information is "no longer required to provide Services". Since PSC has had an agreement with Company X since 2002, it is conceivable that Company X has compiled and managed a great amount of personal information on behalf of PSC. Providing a more specific time period when personal information can or must be destroyed would be beneficial in reducing the risk of a privacy breach. The more personal information retained and the longer it is retained, the more likely an individual's privacy will be breached.

[71] Further, PSC should consider amending its contract with Company X so that Company X is required to notify PSC prior to destroying records. The Government of Alberta's *Managing Contracts under the FOIP Act* states the following:

> As a safeguard against unlawful destruction of records, the public body should consider whether notification of destruction should be required (even when destruction is allowed under the contract). This notification would allow the public body to have the assurance that only records that should be destroyed are destroyed. This is especially important when contracts are of a lengthy duration.[61]

[72] In its letter dated November 15, 2012, my office recommended the above contract amendments to PSC. In its March 22, 2013 letter, PSC provided the following contract

[60] *Supra* note 45.
[61] *Supra* note 41 at p. 70.

language in response to my office's recommendations (which was already partially quoted earlier):

> …
>
> **4. Customer's Instructions**
> During the Services Period of any order for Cloud Services, Customer may provide instructions to [Company X] in addition to those specified in the Agreement with regard to processing of Personal Data. [Company X] will comply with all such instructions without additional charge to the extent necessary for [Company X] to comply with laws applicable to [Company X] as a data processor in the performance of the Services; the parties will negotiate in good faith with respect to any other change in the Services and/or fees resulting from such instructions. [Company X] will inform Customer if, in [Company X's] opinion, an instruction breaches data protection regulations. Customer understands that [Company X] is not obligated to perform legal research and/or to provide legal advice to Customer.
>
> **5. Owner of Data**
> The ownership and control of Personal Data remains with Customer, and Customer will at all times remain the Data Controller. Customer is responsible for compliance with its obligations as data controller under data protection laws, in particular for justification of any transmission of Personal Data to [Company X] (including providing any required notices and obtaining any required consents), and for its decision concerning the processing and use of the data.
>
> **6. Rights of Data Subject**
> [Company X] will grant Customer electronic access to Customer's subscribed Cloud Services Environments that hold Personal Data to permit customer to delete, release, correct or block access to specific Personal Data or, if that is not practicable and to the extent permitted by applicable law, follow Customer's detailed written instructions to delete, release, correct or block access to Personal Data. Customer agrees to pay [Company X's] reasonable fees associated with the performance of any such deletion, release, correction or blocking of access to data. [Company X] shall pass on to the Customer contacts identified in Section 15 below any requests of an individual to delete, release, correct or block Personal Data processed under the Agreement.

[73] The above neither states specific time periods when personal information is to be destroyed nor does it provide any clarity as to how personal information is to be destroyed. The above states that the "Customer" may delete information but the act of deleting information does not necessarily equate to destroying information, especially when information is stored on servers and potentially backup servers. I find that PSC's

response to my office's recommendations in regards to retention and destruction to be inadequate.

c. Use of personal information

[74] As stated above, PSC advised that it had considered the items in the Checklist. The Checklist was created by Saskatchewan Justice pursuant to the Government of Saskatchewan's, *An Overarching Personal Information Privacy Framework for Executive Government*.[62]

[75] What is interesting about the Checklist is that it addresses **collection** and **disclosure** of personal information but it lacks a section that clearly addresses the **use** of personal information. For example, there are sections entitled "Questions about disclosure", "Questions about collection", and "Questions for both collection and disclosure"[63]. I stated in my office's *2004-2005 Annual Report* the following about "use" and "disclosure" in the Checklist:

> There is a lack of clarity and differentiation between "use" and "disclosure". "Use" refers to what happens with personal information when it is utilized in some fashion by a public body, its agents, employees and contractors. A "disclosure" refers to the movement of personal data from the public sector organization to another organization not under the control of the first organization. In other words, a contractor is in no different position for purposes of the FOIP or LA FOIP Acts than an employee working for a public body.[64]

[76] Including a section about "use" in the Checklist would be helpful since I have stated in my office's newsletter, the *Saskatchewan FOIP FOLIO*, that when records are provided to a contractor:

[62] *Supra* note 15 at pp. 23 to 24; The background section of the Checklist states that the creation of the Checklist was a result of *An Overarching Personal Information Privacy Framework for Executive Government*, p. 2, available at www.justice.gov.sk.ca/PICC.
[63] *Supra* note 40 at p. 2.
[64] *Supra* note 16 at p. 29.

> In the privacy world, when records are provided to a contractor and yet remain under the control of a public body this constitutes a "use" and not a "disclosure". In other words, there is no disclosure if the public body retains control over the records.[65]

[77] The above is supported by the OPC, which stated in its publication *Processing Personal Data Across Borders Guidelines*:

> **"Transfer" is a use by the organization. It is not to be confused with a disclosure.** When an organization transfers personal information for processing, it can only be used for the purposes for which the information was originally collected. A simple example is the transferring of personal information for the purpose of processing payments to customers. Or to use another example, an internet service provider may transfer personal information to a third party to ensure that technical support is available on a 24/7 basis. Increasingly, organizations outsource processes to third parties. In many cases, this involves the transfer of personal information. In the context of this document, when we refer to outsourcing, we are referring specifically to outsourcing that involves personal information.[66]
>
> [emphasis added]

[78] A contractor works on behalf of the government institution similar to what would be done by an employee of the government institution. Therefore, since the contractor is working on behalf of the government institution, the transfer of records to the contractor is a "use," not a "disclosure." Through a contract, the contractor uses the information to fulfill the government institution's purpose for collecting the personal information in the first place.

[79] Since I am concerned with the transfer of personal information to contractors, I am concerned with the use of personal information. The lack of a clear use section in the Checklist is not helpful in assisting government institutions to comply with the use provisions of FOIP when contracting with third-party service providers.

[80] Section 7 of the Checklist addresses the fact that the government institution maintains control over the personal information. Section 7 of the Checklist states:

---

[65] *Supra* note 37.
[66] OPC, *Processing Personal Data Across Borders Guidelines*, available at www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf.

> 7. When Personal Information or Personal Health Information is being collected for the government, the contract should make it clear who owns the Personal Information being collected. Unless there is a good reason to the contrary, the information should be the property of the government and a clause should be included in the contract to indicate this.[67]

[81] Further, section 8 of the Checklist states:

> The contract should require the Contractor to:
>
> ...
>
> - not use the information for any purpose other than providing the services[68]

[82] Section 5.2 of the contract between PSC and Company X states that PSC maintains control over the information and that Company X is to only use the information to fulfill contractual duties:

> 5.2 Province Rights
>
> All right, title and interest in and to the Province Data and Deliverables shall remain exclusively with Province and its licensors, as applicable. Except as set forth in Section 2.1(f) or Section 9, without the permission of Province, access to the Province Data is provided to Company X only to allow Company X to fulfill its obligations under this Agreement, including without limitation to diagnose and provide services at Province's request in relation to the site and Platform.[69]

[83] Further, in the amended section 9.2(b) of the contract, it states:

> 9.2 Each party agrees that it will:
>
> ...
>
> (b) **not use the Confidential Information for any purpose other than for the provision of Services under this Agreement. In that regard [Company X] agrees that it will:**
>
> (i) keep Province Data logically separate and apart from other customers information and will not combine the information with any other customers information; and
>
> (ii) only divulge Province Data to those of its officers and employees who require such for the performance of this Agreement and will ensure such

[67] *Supra* note 40.
[68] *Ibid.*
[69] *Supra* note 44.

> officers and employees are aware of and comply with the provisions of this section 9;
>
> [emphasis added]

[84] The use of the personal information appears to be addressed in the contract in spite of the shortcomings of the Checklist.

d. Access to information requests

[85] As stated earlier, section 5 and 31(1) of FOIP provides individuals with the right to access records and their personal information, respectively, in the possession or control of the government institution. Contracts should state that the contractor must assist in the search for responsive records in a timely manner so that the government institution can respond to access to information requests within the legislated timelines. The contract must also state that any records that are responsive to an access to information request must not be destroyed until the request has been responded to and the appeal period of one year has expired, pursuant to section 49(2) of FOIP. Also, the contract should state that any records related to a review or investigation by the OIPC must not be destroyed.

[86] Further, section 32 of FOIP provides individuals the right to request the correction of the personal information in the possession or control of a government institution. Section 32 states as follows:

> **32**(1) An individual who is given access to a record that contains personal information with respect to himself or herself is entitled:
>
> (a) to request correction of the personal information contained in the record if the person believes that there is an error or omission in it; or
>
> (b) to require that a notation be made that a correction was requested but not made.
>
> (2) Within 30 days after a request pursuant to clause (1)(a) is received, the head shall advise the individual in writing that:
>
> (a) the correction has been made; or

> (b) a notation pursuant to clause (1)(b) has been made.
>
> (3) Section 12 applies, with any necessary modification, to the extension of the period set out in subsection (2).[70]

[87] The contract should also specify that if a request for correction of personal information is received by the government institution, that the contractor will cooperate by correcting the personal information or notating that a request to correct the personal information has been made within legislated timelines.

[88] My office communicated the above recommendations to PSC in our letter dated November 15, 2012. PSC provided the following language that will be included in its contract with Company X:

> **6. Rights of Data Subject**
> [Company X] will grant Customer electronic access to Customer's subscribed Cloud Services Environments that hold Personal Data to permit Customer to delete, release, correct or block access to specific Personal Data or, if that is not practicable and to the extent permitted by applicable law, follow Customer's detailed written instructions to delete, release, correct or block access to Personal Data. Customer agrees to pay [Company X's] reasonable fees associated with the performance of any such deletion, release, correction or blocking of access to data. [Company X] shall pass on to the Customer contacts identified in **Section 15** below any requests of an individual to delete, release, correct or block Personal Data processed under the Agreement.[71]
>
> [emphasis added]

[89] PSC did not specify the term "Customer" nor did it provide my office with a copy of "Section 15" referred to in the above contract language. It appears that the above contract language would perhaps enable PSC to locate and retrieve information in response to access to information requests and/or correction requests.

[90] The above contract language, though, does not adequately address the destruction of personal information in accordance with retention and destruction schedules, as discussed

[70] *Supra* note 4 at section 32.
[71] Enclosed with memorandum dated March 22, 2013 from PSC to the SK OIPC.

earlier in this Report.[72] In the event of an active review or an active investigation by my office, PSC needs to ensure that relevant records are not destroyed. I recommend that PSC amend its contract with Company X to address such a scenario.

e. Safeguards

[91] Section 28 of FOIP states that a government institution must not use personal information under its control without proper authority. Similarly, section 29 of FOIP states that a government institution must not disclose personal information in its possession or under its control without authority. In order to comply with the two provisions, a government institution must have physical, technical and administrative safeguards in place to ensure as much as possible that personal information will not be used or disclosed without proper authority.

[92] Section 16 of HIPA imposes the duty to protect upon trustees as follows:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.[73]

[72] I discussed retention and disposition of records at [68] to [73].
[73] *Supra* note 48 at section 16.

[93] I note that FOIP does not have a provision such as the one above but nonetheless, the duty to protect information from improper use or disclosure is implied through sections 28 and 29 of FOIP.[74]

[94] In regards to security, the Checklist provides as follows:

> …
>
> **5.** The Contractor needs to be able to protect the information provided.
>
> **What is the level of protection that you expect? It should not be any less than the level of protection which you use to protect the information within your Government Organization. Consider the following:**
>
> **5.1** Does the Contractor have proper polices [sic] and procedures restricting access to this information only to its employees with a need to know the information?
>
> Yes_____ No_____
>
> A copy of the policies and procedures should be retained.
>
> **5.2** Does the Contractor have a process to be able to identify who accessed the information?
>
> Yes_____ No_____
>
> **5.3** Does the Contractor have a process which will immediately remove the ability of former employees to access information?
>
> Yes_____ No_____
>
> **5.4** The USA Patriot Act could enable the USA government to obtain information which is stored, processed or transmitted into the USA or which is in the control of an American corporation. The USA Patriot Act could compel the Contractor to disclose Personal Information, notwithstanding any contractual commitment to keep it confidential. Accordingly, if the Act does apply to the Contractor, consideration should be given as to whether the Government Organization wants to accept that risk, given the nature of the information at issue, or not use that Contractor.
>
> Are you satisfied that the contractor is not an American corporation and that the information will not be stored, transmitted or processed (by the contractor or a

[74] *Supra* note 10 at [89], I made a similar comment with respect to FOIP.

subcontractor) in the USA and/or, if it is potentially subject to the USA Patriot Act are you willing to accept the potential risk?

Yes_____ No_____

5.5 Have you discussed the previous four questions with the Contractor and are you satisfied that the Contractor can meet the security level that is expected?

Yes_____ No_____

IF NO - then you shouldn't enter into the contract.

6. Are you satisfied that the Contractor has no criminal background which might cause concern in the Contractor having this information? If the Contractor is a corporation, does it have a criminal record check (CRC) policy for its employees? You should be aware that CRCs are required for Contractors (or their employees) who deliver services which, if delivered by a government employee, the government employee would be required to have a CRC.

Yes_____ No_____

IF NO – you shouldn't proceed with the contract.[75]
...

[emphasis added]

[95] The Checklist states that the overall question is "What is the level of protection that you expect? It should not be any less than the level of protection which you use to protect the information within your Government Organization."[76]

[96] PSC did not particularize for my office the level of protection it expected from PSC or from Company X. Therefore, it was difficult to conclude how it evaluated Company X's security policies and procedures to determine that they were adequate when negotiating its contract with Company X. However, since PSC is subject to FOIP, then as PSC's contractor, Company X should be managing personal information in accordance with FOIP.

[75] *Supra* note 40.
[76] *Ibid.*

[97] In its submission to my office, PSC provided us with copies of Company X's Information and Security Policies and Procedures, including:

- *Computer Security Incident Handling*,
- *Information Security Breach Notification Policy*,
- *Production Data Management Policy*,
- *Secure Computer Use Agreement*,
- *Corporate Information Security Policy* (CISP), and
- [Company X] *Backup & Recovery Program Overview*.

[98] Policies and procedures can be ever-changing. Certainly, it appears that Company X's policies and procedures are extensive. However, the contract between PSC and Company X does not appear to have a provision that binds Company X to operate in accordance with such policies and procedures. Now, the contract should state that there be no assignment of the contract without the prior express consent of PSC. PSC has not provided my office with any evidence it has ensured contractually that Company X will maintain its security policies and procedures in such a way that meets PSC's expectations.

[99] In my office's letter dated November 15, 2012, my office recommended that PSC make clear what its own internal security standards and practices are. Once it has made such a determination, then it should evaluate Company X's security policies and procedures against PSC's own internal security standards and practices and determine if there are any gaps that should be addressed. PSC should include a provision that binds Company X to concrete and specific security standards and practices. Further, my office recommended that PSC include in its contract provisions what the responsibility of the other contracting party (Company X, in this case) is if and when the other contracting party is purchased by another entity, including a requirement to notify PSC of the purchase.

[100] PSC responded to my office's recommendation to identify its own internal security standards and practices, in a letter dated March 22, 2013 by stating the following:

> …please see the non-master services contract template (attachment B). This is the standard the government uses, including PSC, as a basis for negotiating all

> information technology contracts. **It was used to assess the security standards of the 2013 contract with [Company X].**
>
> [emphasis added]

[101] Unfortunately, PSC did not provide me with the results of its assessment when it reviewed the "non-master services contract template" or the IT service agreement template to assess Company X's security policies and procedures. Further, I note that there were very general statements in regards to keeping information confidential or complying with security policies and practices but no specific description of those security policies and practices. For example:

> **5.0 CONFIDENTIALITY**
>
> **5.1** All information, documents, data, software and other Client information or Supplier information as the case may be, including passwords and personal information within the meaning of The Freedom of Information and Protection of Privacy Act and personal health information within the meaning of The Health Information Protection Act, whether in paper, electronic or other form ("the Confidential Information") which is provided to or obtained by one party from the other party in the course of performing Services shall be treated and maintained by the receiving party as confidential. **Each party shall safeguard the Confidential Information of the other using the same standard or [sic] care, but not less than a reasonable standard of care, the party uses to protect its own Confidential Information and materials.** One party will not disclose the Confidential Information of the other except for the following:
> …
>
> **5.3 While the Supplier provides Services at the Client's premises the Supplier shall comply with the Client's information security policies and practices applicable to the Client premises, provided the Supplier has received notice of the same.** Officers and employees of the Supplier, its contractors and agents will be subject to the same electronic monitoring as government employees while on the Client's premises. Client Confidential Information shall only be removed from the Client's premises by the Supplier if, and to the extent necessary to perform the Services, and only with the prior knowledge and consent of the Client.[77]
>
> [emphasis added]

[77] *Supra* note 71.

[102] The reference to how the contractor treats its own confidential information is not helpful. My concern is the standard for protecting personal information and personal health information of PSC.

[103] I find that what purports to be the security standards requirements in the IT service agreement template is quite skeletal. It is unclear how the above could be used to evaluate Company X's security policies and procedures, including the ones listed at [97].

[104] Further in its March 22, 2013 letter, PSC provided the language that deals with assignment of the contract to a third party. The new contract language provided is as follows:

> **Assignment.** Neither party may transfer or assign this Agreement, including by merger or operation of law, without the other party's prior written consent, except (i) to a successor in interest following a merger or other change of control, or (ii) to an Affiliate upon receipt of thirty (30) days notice from the assigning party. In the event an Affiliate to which the Agreement is assigned fails to meet its obligations under the Agreement, the assigning party shall remain liable for such obligations.

[105] The clause (ii) above is unclear. Otherwise, the above amendment appears to address in part one of my office's recommendations regarding assignment of the outsourcing contract.

f. Audit Provisions

[106] In regards to auditing, the Checklist provides the following:

> The contract should require the Contractor to:
> ...
> - permit you to audit the Contractor's security practices.[78]

[107] Further, the British Columbia IPC has made recommendations in its *Privacy and the USA Patriot Act Implications for British Columbia Public Sector Outsourcing* in addressing

[78] *Supra* note 40.

privacy risks when contracting for services that involve the collection, use, or disclosure of personal information. One of the recommendations is as follows:

> Recognizing that it is not enough to rely on contractors to self-report their breaches, a public body that has entered into an outsourcing contract should create and implement a program of regular, thorough compliance audits. **Such audits should be performed by a third party auditor, selected by the public body, that has the necessary expertise to perform the audit and recommend any necessary changes and mitigation measures.** Consideration should be given to providing that the contractor must pay for any audit that uncovers material noncompliance with the contract.[79]
>
> [emphasis added]

[108] My office reviewed the contract that was between PSC and Company X and it appeared that there were no auditing provisions that enabled PSC to audit Company X to ensure compliance with the contract.

[109] PSC stated the following in its letter dated February 28, 2012 to my office:

> 2. [Company X] Audit Reports
>
> No documentation was located regarding an assessment focused particularity on privacy prior to signing of the 2002 and 2006 contracts. However, IT security risks were assessed, as indicated in the RFP assessment process (see Tab 8) and the 2002 contract (see Tab 2). Further, in 2008, [Company X] hired an independent auditor to audit their practices against their policies in their American facilities: Independent Service Auditor's Report on Controls Placed in Operation and Tests of Operation Effectiveness, [name of auditing company], Certified Public Accountants, (April 1, 2008 to September 30, 2008) (see Tab 9). According to their web site at [website link], in January 2011, [name of auditing company], one of the world's largest providers of [name of auditing company] audit services, changed its name to [new name of auditing company]."[New name of auditing company] is a licensed Certified Public Accounting firm and is registered with the Public Company Accounting Oversight Board…
>
> The detailed auditor's report assessed [Company X's] performance in the areas of control environment, risk assessment, monitoring, information and communication systems, physical security, environmental security, computer operations, information security, application change management and data communications. No relevant exceptions were identified.

[79] Supra note 12 at p. 20.

[110] Based on the above, it appeared that PSC did not undertake its own audits of Company X to ensure that Company X was complying with contractual obligations. Therefore, my office recommended in its letter dated November 15, 2012 that PSC amend the contract so that PSC has the ability to audit Company X to ensure that Company X is fulfilling contractual obligations.

[111] PSC responded in its letter dated March 22, 2013 and provided my office with the following contract language that is intended to be used in the new contract between PSC and Company X:

> **10 Audit Rights**
>
> Customer may audit [Company X's] compliance with the terms of the Agreement and this Data Processing Agreement up to once per year. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and [Company X] and must execute a written confidentiality agreement acceptable to [Company X] before conducting the audit. To request an audit, Customer must submit a detailed audit plan at least two weeks in advance of the proposed audit date to [Company X's] Global Information Security organization ("GIS") describing the proposed scope, duration, and start date of the audit. [Company X] will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise [Company X] security, privacy, or employment policies). [Company X] will work cooperatively with Customer to agree on a final audit plan. The audit must be conducted during regular business hours at the applicable facility, subject to [Company X] policies, and may not unreasonably interfere with [Company X] business activities. If the information required for such an audit is not contained in a SSAE 16/ISAE 3402 Type 2 or similar report, [Company X] will make reasonable efforts to provide requested information to the auditor.
>
> Customer will provide GIS any audit reports generated in connection with any audit under this section, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements by law. Customer may use the audit reports only for the purposes of meeting it regulatory audit requirements and/or confirming compliance with the requirements of the Agreement and this Data Processing Agreement. The audit reports are Confidential Information of the parties under the terms of the Agreement. Any audits are at the Customer's expense. Any request for [Company X] to provide assistance with an audit is considered a separate service if such audit assistance requires the use of different or additional resources. [Company X] will seek the Customer's written approval and agreement to pay any related fees before performing such audit assistance.

[112] PSC did not provide explanations for terms used above, including "Customer". Assuming that "Customer" refers to PSC, it appears that the above contract language will enable PSC to audit Company X to ensure it is complying with the terms of the contract.

g. Subcontracting

[113] Just as PSC has stated in its submission, FOIP does not prohibit the transfer of personal information outside of Canada. However, even if a contractor was situated in Canada, the contractor could subcontract services which could potentially mean the transfer of personal information outside of Canada. If the government institution determines that a contractor may subcontract, the contract should specify what services can be subcontracted. The British Columbia IPC states the following in regards to subcontracting:

> …
>
> 5. The public body should carefully consider whether the contractor should be allowed to sub-contract any services under the contract. If sub-contracting is allowed, only qualified sub-contractors should be permitted. The contractor should be required to ensure that any sub-contract requires the sub-contractor to comply with the privacy provisions of the contract between the contractor and the public body. **The public body should consider requiring the contractor to get the public body's express, written approval of sub-contract provisions before the subcontract is signed, with the public body having the discretion to refuse approval if it reasonably considers the proposed sub-contractor does not have the experience and capacity to perform the sub-contract.**[80]
>
> …
>
> [emphasis added]

[114] The Alberta IPC stated its concern over subcontracting as follows:

> 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.

[80]BC IPC, *Guidelines for Data Services Contracts: OIPC Guideline 01-02*, May 8, 2003, at p. 5, available at www.oipc.bc.ca/advice/Guidelines-Data_services.pdf.

> 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…[81]

[115] The following provision in the PSC and Company X contract appears to speak to subcontracting:

> 9.3 If to provide the Services [Company X] must disclose or make accessible any Province Data to a third party, before doing so [Company X] will obtain from the third party a written agreement under which the third party agrees to be bound by confidentiality obligations at least as restrictive as those contained in this section 9 applicable to [Company X].[82]

[116] Further, the following provision allows for Company X to have its own contractors:

> 5 Section 10 is amended as follows:
>
> (a) by deleting the current provision entirely and replacing section 10.1 with the following:
>
> This Agreement shall be effective February 1, 2010 through January 31, 2013.
>
> (b) by adding the following to section 10.2:
>
> The Province may immediately terminate this agreement by written notice to [Company X] should [Company X], **its contractors or agents** breach any provision of sections 9 or 9A.[83]
>
> [emphasis added]

[117] The above provisions do not require Company X to notify PSC if Company X subcontracts any of the services it delivers to PSC. Effectively, excluding PSC from the subcontracting process hinders and disables PSC's ability to maintain control over the information. For example, as far as PSC is aware, the information is transferred and stored in the USA. However, if Company X subcontracts with another company to store

[81] *Supra* note 24 at p. 28.
[82] *Supra* note 44.
[83] *Supra* note 45.

the information, the information can be transferred to yet another jurisdiction and therefore, subject to further foreign legislation.

[118] Further, PSC's collection notice during the course of this investigation appeared as follows. It only notified job applicants that their personal information will be stored in the USA.

> Please be aware that the information in your application will be stored electronically on a server in the U.S.A. The information will be protected with **appropriate security safeguards**, but may be subject to U.S. laws.[84]
>
> [emphasis added]

[119] Since I have stated that imposing the duty to protect through legislative reform of FOIP is an essential safeguard, then PSC's position that there are appropriate security safeguards is inaccurate. Without the legislated duty to protect, PSC should provide clear notification to all affected individuals, be they employees or job applicants, that there currently is not adequate protection for employees or job applicants when their personal information is collected, used or disclosed outside of Canada.

[120] Conceivably, Company X can subcontract storage services of personal information without notifying PSC under the current contract. Therefore, personal information may be stored anywhere in the world, not simply in the USA. In order for PSC to remain in control of the personal information, any subcontracts that Company X is contemplating should be approved by PSC before the subcontract is entered into that would enable PSC to be aware and contemplate further risks to the personal information. If the personal information will be stored outside of the USA by Company X or a subcontractor, PSC must revise its collection notice to notify job applicants of where their information will be stored.

[121] My office recommended in its letter dated November 15, 2012 that PSC modify provision 9.3 that requires Company X to not only notify PSC if it wishes to subcontract services

[84]This appears in the "Privacy Agreement" that appears before job applicants after they have clicked on "Apply Online" of a job advertisement on PSC' Careers website: www.careers.gov.sk.ca/publicjobs.

but that PSC must approve of any subcontracts before Company X moves forward with executing a subcontract. PSC must ensure that subcontractors are also managing personal information in compliance with Part IV of FOIP. Further, my office's letter recommended that PSC provide clear notification to all affected employees and job applicants that without an explicit duty to protect in FOIP, there is not adequate protection for employees and job applicants.

[122] As a part of its March 22, 2013 letter, PSC provided my office with the contract language it is intending to use in its new contract. The language is as follows:

> **8. Affiliates and Subcontractors**
>
> **Some or all of [Company X's] obligations under the Agreement may be performed by [Company X] Affiliates.** [Company X] and the [Company X] Affiliates have subscribed to the intra-company agreement specified above, under which an [Company X] subsidiary handling Personal Data adopts safeguards consistent with those of the [Company X] subsidiary contracting with a customer for [Company X] Cloud Services. The [Company X] Affiliate contracting with the customer is responsible for [Company X] compliance and the [Company X] Affiliates' compliance with this requirement. [Company X] also may engage third party subcontractors to assist in the provision of the Services and such subcontractors may have access to Personal Data. **[Company X] maintains a list of subcontracts that may have access to Personal Data of [Company X's] Cloud Service customers and will provide a copy of that list to the Customer upon request.**
>
> All subcontracts are required to abide by substantially the same obligations as [Company X] under this Data Processing Agreement as applicable to their performance of the Services. **Customer may request that [Company X] audit the subcontractor (or, where available, obtain or assist customer in obtaining a third-party audit report concerning subcontractor's operations) to ensure compliance with such obligations. Customer also will be entitled, upon written request, to receive copies of the relevant terms of [Company X] agreement with subcontractors with access to Personal Data**, unless the agreement contains confidential information, in which case [Company X] may provide a redacted version of the agreement. [Company X] shall remain responsible at all times for compliance with the terms of the Agreement and this Data Processing Agreement by [Company X] Affiliates and subcontractors. **Customer consents to [Company X's] use of [Company X] Affiliates and subcontractors in the performance of the Services in accordance with the terms of Sections 7 and 8 above.**

[emphasis added]

[123] Further, in its letter dated March 22, 2013 to my office, PSC stated that it is "confident that the data will be protected the same as if there was a duty to protect under the Act, and therefore, the warning would not be necessary or informative." I disagree for reasons outlined earlier.

[124] My office was not provided a copy of "section 7" referred to in the above contract language. Therefore, I cannot evaluate on what basis PSC consents to Company X using "Company X Affiliates and subcontractors". The above suggests that Company X will use affiliates and contractors and that PSC may, upon request, learn with whom Company X has contracted with and the terms of Company X agreements with subcontractors. PSC does not have the option of approving or disapproving with whom Company X subcontracts. Based on the information provided to my office, PSC is effectively powerless in determining with whom Company X may subcontract and share PSC's information. I find that section 8 of the contract language (quoted above) is inadequate in meeting my office's recommendation that PSC must approve of subcontracts before Company X shares any of PSC's information with a subcontractor.

[125] In regards to PSC's response to my office's recommendation to provide clear notification, to respect the privacy of individuals in this province, individuals should be provided notification that FOIP lacks the explicit duty to protect and therefore, there is inadequate protection of their personal information.

[126] Privacy is the right of the individual to exercise a measure of control over how his or her personal information is collected, used, or disclosed. Not only should individuals be informed that their personal information may be stored electronically in the USA, but that it may be stored and/or processed in jurisdictions outside of Canada or the USA. Given that this investigation was initiated by Ministry A's staff concerns over their personal information being stored in the USA and subject to the USA PATRIOT Act, it would be logical to conclude that staff and other affected individuals would be interested in being notified that their personal information may be subject to further foreign jurisdiction.

d. Privacy Impact Assessment

[127] In its submission dated February 28, 2012, PSC stated the following:

> 5. When the [Company X] contract was renewed again in 2010, further precautions were taken by the PSC. Prior to signing the 2010 agreement, a team of government employees, which included the two PSC employees who are responsible for signing the agreement and operating the [Company X] system for/at the PSC, one employee from the Information Technology Office (ITO), and the PSC Privacy Officer, together conducted a review of the risks to the data to inform the then upcoming renewal of the agreement with [Company X] (see Tab 10):
>
> **a. The ITO's Project Privacy Evaluation (see Tab 10, first section)**
> b. The Personal Information Contract Checklist (see Tab 10, second section)
> c. A summary of the results of the Personal Information Contract Checklist and subsequent enhancements to the contract (see Tab 10, third section)
>
> [emphasis added]

[128] The completed Information Technology Office (ITO) Project Privacy Evaluation form noted above was provided to my office. It reads as follows:

> **Privacy Evaluation for <insert Project Name>**
>
> **Directions for using template:**
>
> Read the Guidance (Arial blue font in brackets) to understand the information that should be placed in each section of this template. Then delete the Guidance and replace the placeholder within <<Begin text here>> with your response. There may be additional Guidance in the Appendix of some documents, which should also be deleted once it has been used.
>
> Some templates have three levels f [sic] headings. They are not indented, but can be differentiated by font type and size:
>
> Heading 1 – Arial Bold 12 font
> Heading 2 – Arial Bold 10 font
>
> Heaing 3 – Arial Italic 10 font
>
> You may elect to indent sections for readability.
>
> **[Description**: This template is to be used on all projects to complete an initial privacy assessment. After completing the assessment, contact the Client/Sponsor for the

project to have this assessment communicated to the Client/Sponsor's Privacy Officer. **The privacy assessment is typically completed during the inception phase of a project to ensure personal and personal health information is identified and reflected in the solution design and adequate time is estimated.]**

Description of Project
[Insert a brief description of the project]

Part 1: Privacy Evaluation
[Description: a Privacy Impact Assessment (PIA) ensures compliance with the fundamental privacy principles of the Privacy Framework, *The Freedom of Information and Protection of Privacy Act* (applies to "Personal Information" in government) and *The Health Information Protection Act* (applies to "Personal Health Information" in government). Complete the following checklist. **If any of the information noted is within the scope of the project, a formal PIA should be undertaken and appropriate time and resources estimated.** Please contact the Client/Sponsor's Privacy Officer for instructions on how to proceed.]

Personal Information	In Project Scope	Out of Project Scope
Race, Creed, Religion, Colour, Sex, Sexual Orientation, Family/Marital Status, Disability, Age, Nationality, Ancestry, or Place of Origin	✓	
Education, Criminal or Employment History, or Financial Transactions	✓	
Identifying number, symbol, or other particular assigned to the individual (other than the individual's health services number as defined in *The Health Information Protection Act)* (e.g. S.I.N. #)	EE #	
Personal opinions or views of the individual (except where they are about another individual)	✓	
Correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would	✓	

reveal the content of the original correspondence		
Views or opinions of another individual with respect to the individual	✓	
Information that was obtained on a tax return or gather for the purpose of collecting a tax.		✓
Information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness		✓
Name of the individual where it appears with other personal information that relates to the individual	✓	
Name of the individual where the disclosure of the name itself would reveal personal information about the individual.		✓

The following information is not personal information although it may be considered confidential and/or sensitive and may require appropriate processes and/or security to protect the data.

Non-Personal Information	**In Project Scope**	**Out of Project Scope**
The classification, salary, discretionary benefits or employment responsibilities of an individual who is or was an officer or employee of a government institution or a member of the staff of a member of the Executive Council;	✓	
The salary or benefits of a legislative secretary or a member of the Executive Council		✓
The personal opinions or views of an individual employed by a government	✓	

institution given in the course of employment, other than personal opinions or views with respect to another individual		
Financial or other details of a contract for personal services		✓
Details of a license, permit or other similar discretionary benefit granted to an individual by a government institution		✓
Details of a discretionary benefit of a financial nature granted to an individual by a government institution		✓
Expenses incurred by an individual travelling at the expense of a government institution		✓

The following is considered personal health information protected under HIPA. **If any of this information is in the scope of your project, a Privacy Impact Assessment should be considered.**

Personal Health Information	**In Project Scope**	**Out of Project Scope**
Personal health information with respect to • the physical or mental health of the individual • any health service provided to the individual • the donation by the individual of any body part or bodily substance • providing health services to an	✓	✓

individual or incidentally to the provision of health services • registration information		

Completed by [name of employee] January 11/2010

[emphasis added]

[129] As noted above, the ITO states that if personal information or personal health information is determined to be "in project scope", then a formal Privacy Impact Assessment (PIA) should be completed. However, it appears that PSC never undertook a PIA even though it is clear that personal information and personal health information is collected by PSC.

[130] Further, this ITO Project Privacy Evaluation form certainly recognizes that personal information and personal health information are distinctly different from other types of information. However, PSC aggregates personal information and personal health information with other types of information to be known collectively as "confidential information" in its contract with Company X. It appears the completion of this form made minimal difference to the text employed in the contract with Company X.

[131] ITO's Project Privacy Evaluation form suggests a PIA should be completed to ensure compliance with access and privacy legislation in the province. In the January 2006 edition of my office's publication, the *Saskatchewan FOIP FOLIO*, I stated the following about PIAs:

> A Privacy Impact Assessment (PIA) is a diagnostic tool designed to help organizations assess their compliance with the privacy requirements of Saskatchewan legislation. On our website under the *Resources* tab, you will see that we are now offering three new PIA questionnaires specific to each of the provincial laws that our office oversees. Accompanying each statute-specific PIA on our website is a

> customized worksheet containing checkboxes and a notes section for documenting responses to questions posed in the questionnaire.
>
> Conducting a Privacy Impact Assessment requires more than just assigning one individual responsibility for completing the questionnaire. **The PIA process involves mapping personal information flows (internally and externally). It also takes you through a set of questions to assist in identifying the privacy risks.** It is usually valuable to involve your Privacy Officer or FOIP Coordinator in the preparation of the PIA and not just those individuals actually designing the new system, policy, procedure or program.
>
> For a sampling of excellent PIA materials from other Canadian and International jurisdictions, follow this link: http://www.ipc.on.ca/docs/phipa_pia-e.pdf[85] to Appendix B on Page 35 of the document.[86]
>
> [emphasis added]

[132] My office wrote a letter dated October 27, 2009 to PSC requesting more information regarding how it assessed risk and action taken to mitigate risks. PSC responded as follows:

> Q5: *In terms of safeguarding the survey information, the cover page reads as follows: "Please note that the information collected in this survey will be treated as confidential and will only be used to determine redeployment options so that priority programs remain operational. Access to the survey information will be limited to those involved in contingency planning, and the data will be stored in a secure database." We are unclear how the Ministry arrived at the above conclusion without first having undertaken a formal assessment of risk and taken remedial action to mitigate said risks (October 27, 2009 letter from OIPC, page 4).*
>
> **The PSC was satisfied with the security measures in the database based on the extensive [Company X] security policies and procedures and PSC user level security for access to the survey data. Access to the data was granted on a need-to-know basis by a System Administrator. Only System Administrators are given the security access and ability to view all data, make changes to the system configuration, and determine and grant access to other users. There are three PSC employees with this level of access.**
>
> For purposes of the survey, the PSC created a user type (the particular level of access given to a user for Emergency Preparedness Officers (EPO) – one or two per ministry. This user type gave the EPOs access to survey data for employees in their own ministries only. There was also a central coordination office (approximately

[85]This link has since been updated to www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf.
[86]SK OIPC, January 2006 *Saskatchewan FOIP FOLIO*, available at www.oipc.sk.ca/FOIPFOLIO/January2006.pdf.

> three individuals, all PSC employees); these individuals had access to all survey data. The purpose for central coordination was the facilitate re-deployment of employees across ministries.
>
> The system uses [granular security detail], and times out after [granular security detail] of inactivity for users. In addition to this, there is the system-lock that occurs on each Information Technology office (ITO) hosted computer after a period of inactivity.
>
> [emphasis added]

[133] Certainly, ensuring that Company X has its own security policies and procedures is a good measure. However, although security is a concept related to privacy, it is not synonymous with privacy. Security is the measure taken to ensure personal information or personal health information is not exposed to individuals who should not have access. Examples of security measures are passwords, encryption of information, locked filing cabinets, etc. As stated earlier, privacy is the right of the individual to exercise a degree of control over how his or her personal information is collected, used, and disclosed. Therefore, it is not adequate to simply rely on the contractor's security policies and procedures to expect compliance with our provinces' access and privacy legislation.

[134] In my office's letter dated November 15, 2012 to PSC, I recommended that PSC undertake a comprehensive PIA to ensure the information collected, used and disclosed with Company X, or with any other contractor, is in compliance with FOIP.

[135] On December 14, 2012, my office received a call from PSC. It stated that it was in negotiations with Company X for a new contract since its then-current contract expired at the end of January 2013.

[136] In telephone calls between my office and PSC on February 28, 2013 and March 1, 2013, PSC advised that it would complete a PIA but only **after** it completed negotiations and entered into a new contract with Company X.

[137] My office's position was that the PIA ought to be completed prior to entering into a new contract. The value of a PIA is in its findings and results. Such findings and results could be used as part of the negotiations of the new contract.

[138] A Portfolio Officer from my office and I met with two Assistant Chairs of PSC on March 18, 2013. They both explained that Company X was central to its staffing system and they lacked the time to complete a PIA prior to entering into a contract. They stated the length of the contract would be for two years. However, in the meantime, it would complete a PIA, so when the newly signed contract expires, it would be able to negotiate a new contract taking into consideration the PIA's findings and results. PSC re-iterated its position as follows in its letter dated March 22, 2013 to my office:

> Regarding the recommendation to undertake a formal privacy impact assessment (PIA) to ensure that [Company X] is in compliance with *The Freedom of Information and Protection and Privacy Act* and *The Health Information Protection Act*, the PSC will endeavour to have it completed by March 31, 2014. As we noted in our March meeting, the [Company X] system is critical to staffing positions in government, so we felt we could not hold the signing of the contract until after the PIA was complete.

[139] It is disappointing that PSC is apparently entering into a new contract without first cataloguing and analyzing the privacy risks. PIAs are an important tool to use to not only determine how well a program complies with the applicable access and privacy law and privacy best practices, but it also assists government institutions to identify privacy risks and measures to mitigate such risks. The PIA would be a road map for a government institution to follow in activities such as negotiating contracts with service providers.

IV FINDINGS

[140] I find that *The Freedom of Information and Protection of Privacy Act* does not prohibit the transfer of personal information to outside of Canada.

[141] I find that though the 2010 amendments made to the contract between the Public Service Commission and Company X address some privacy issues, a number of amendments should still be made.

[142] I find that intended language that will be used for section 8 of the new contract between the Public Service Commission and Company X is inadequate in meeting my office's recommendation that the Public Service Commission must approve of subcontracts before Company X shares any of the Ministry of Central Service's information with a subcontractor.

[143] In the absence of a legislated requirement to safeguard personal information, there is significant risk to privacy that is not reasonably addressed by the contract between the Public Service Commission and Company X, and by the collection notice provided to job applicants.[87]

[144] I find that the Information Technology service agreement template provided to my office is too vague and general to allow an open assessment of security policies and procedures for service providers.

V RECOMMENDATIONS

[145] I recommend that the Public Service Commission clearly determine and document its own security standard and practices, which should be in accordance with what *The Freedom of Information and Protection of Privacy Act*, *The Health Information Protection Act, An Overarching Personal Information Privacy Framework for Executive Government*, and privacy best practices requires. Once that determination and

[87] *Supra* note 84.

documentation is made, then it evaluate the security policies and practices of Company X to ensure that Company X is meeting what *The Freedom of Information and Protection of Privacy Act* requires.

[146] I recommend that the Public Service Commission amend the contract it has with Company X so that the contract provides specific time periods when information may be destroyed.

[147] I recommend that the Public Service Commission amend the contract it has with Company X to state who is responsible for the destruction of records and how the records should be destroyed. If Company X is responsible for the destruction of records, the contract should be amended so that Company X notifies the Public Service Commission before it destroys the records.

[148] I recommend that the Public Service Commission amend the contract it has with Company X to state that no records related to an access to information request or a request for correction can be destroyed while the request is being processed, or within the appeal period of one year. Further, no records should be destroyed if it is related to an active review or active investigation by the Office of the Saskatchewan Information and Privacy Commissioner.

[149] I recommend that the Public Service Commission amend the contract it has with Company X so that the Public Service Commission must provide prior approval of any assignment or subcontract Company X is contemplating that would affect the personal information of Saskatchewan residents.

[150] I recommend that the Public Service Commission undertakes a formal privacy impact assessment to ensure that it is in compliance with *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act* prior to entering into a new contract with Company X that would replace the contract that expired in January 2013.

[151] I recommend that the Public Service Commission provide clear notification to all affected employees and job applicants that without an explicit duty to protect in *The Freedom of Information and Protection of Privacy Act*, there is inadequate protection for the privacy of employees and job applicants.

[152] I recommend that the Government of Saskatchewan amend *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act* so that they include an explicit duty to protect the personal information in the possession or control of public bodies.

Dated at Regina, in the Province of Saskatchewan, this 28th day of August, 2013.

R. GARY DICKSON, Q.C.
Saskatchewan Information and Privacy Commissioner