# Protecting Saskatchewan data—the *USA Patriot Act*

# 20

## Main points

On June 6, 2011, the Standing Committee on Public Accounts (PAC) asked that:

> ...when the Provincial Auditor next reports that they take a look at all of the necessary protections that ITO has in place to ensure the citizens of Saskatchewan that their third party contractor cannot share information with the parent company where the parent company is subject to the Patriot Act.

The *USA Patriot Act* does not represent the only risk for Canadian data. And while PAC's motion was in regards to ITO's third party contractor, the same risks are applicable wherever a government agency uses a service provider that stores or processes data in the US, is a US corporation itself, or has a corporate parent in the US. There are also many different ways that agencies can end up with data at risk.

Agencies can manage risks by assessing the risks of using third party contractors, considering risks when selecting contractors, and putting adequate protections in contracts. ITO had some protections in place. Although we make recommendations for how those protections could be improved, these protections can only manage risk, not eliminate it.

Because of security weaknesses at ITO reported in Chapter 16, the protections may not be effective in achieving their intended purpose.

A further way of protecting Saskatchewan data is through the law. 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.

## Introduction

This chapter sets out the results of our study into how the Information Technology Office (ITO) protects data that is managed and stored for it by a service provider, where the service provider might be required by United States (US) law to provide that data to a US law enforcement agency. We undertook this study at the request of the Standing Committee on Public Accounts (PAC).

While PAC's motion was in regards to ITO's third party contractor, the same risks are applicable wherever a government agency uses a service provider that stores or processes data in the US, is a US corporation itself, or has a corporate parent in the US. In this chapter we outline the implications of the *USA Patriot Act*[1] for ITO and other government agencies and describe how the related risks can be managed.

## Standing Committee on Public Accounts motion

On June 6, 2011, PAC passed the following motion:

> That when the Provincial Auditor next reports that they take a look at all of the necessary protections that ITO has in place to ensure the citizens of Saskatchewan that their third party contractor cannot share information with the parent company where the parent company is subject to the *Patriot Act*.[2]

## Our response to the motion

The protections put in place by ITO cannot ensure that information will not be accessible through the operation of the *USA Patriot Act*. Short of a decision to exclude the third party contractor because of its corporate ownership, ITO's contractual protections represent a reasonable attempt to manage risks related to the *USA Patriot Act*.

However, as discussed in Chapter 16 – Information Technology Office, our audit of IT security at ITO has identified security weaknesses. These security weaknesses relate to the information managed by the third party contractor. Until these weaknesses are addressed, government

[1] The text and legislative history of the *USA Patriot Act* can be found at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:H.R.3162:.

[2] http://docs.legassembly.sk.ca/legdocs/Legislative Committees/PAC/Minutes/PAC_35_Minute_June_6_2011.pdf.

information is at risk of inappropriate access or modification. As well, until ITO monitors whether security requirements that the third party contractor needs to follow are being met, the contractual protections may not be effective in achieving their intended purpose.

In addition, a further means of protecting data is through legislation. We recommend in this chapter that the Ministry of Justice and Attorney General work with the Office of the Information and Privacy Commissioner to address the Commissioner's recommendations for changes to Saskatchewan's access and privacy laws.

In the following sections, we outline the risks related to the *USA Patriot Act* and describe how these risks are managed.

## ITO, its service provider, and the data centre

ITO delivers goods and services related to information technology (IT) to ministries and government agencies. It sets policies and standards for the Government of Saskatchewan respecting IT and information management. Its responsibility for doing so is set out in its regulation.[3]

As part of delivering IT goods and services, ITO uses a data centre, which is a central location for computer network hardware and software, especially storage devices for data. Due to the extensive use of IT in managing government and delivering government programs and services, the ITO data centre contains significant amounts of information. This includes sensitive and confidential information. ITO is responsible to protect the information that it manages, whether directly or through a service provider.

Effective December 6, 2010, ITO commenced an agreement with a service provider to operate and maintain its data centre until December 5, 2017. The service provider, through multiple levels of ownership, is a subsidiary of a US company.

[3] *The Information Technology Office Regulations, 2007*, s. 3.

## What is the impact of the *USA Patriot Act*?

The *USA Patriot Act* made numerous amendments to US laws. The effect of those amendments includes permitting US law enforcement agencies to require US persons or entities to furnish information. Those orders can apply to information that is in the US, Canada, or elsewhere. A US company can be ordered to provide information that exists (for example on a computer server) in the US. But the US company can also be ordered to provide information to which it has access even if that information is in Canada. The US company subject to the order is not permitted to reveal the existence of the order or that it provided information.

## What kinds of data are at risk?

There are risks involved in storing electronic information anywhere that is not under your direct control. Increasingly, people, businesses, and governments are giving their data to others to manage and store. In this chapter we are focusing on the use of a contractor to operate a data centre. But other situations where data is at risk include:

- Email services, social media, and back up sites
- Services that store information and copies of documents so users can access them from wherever they have access to a computer and the Internet, such as Google Docs, Microsoft Office 365, and Apple iCloud
- Web-based applications where third parties manage the systems and/or host the data
- Other instances of cloud computing where users pay for computing services provided by others over the Internet

In addition, vendors of IT services are often given access to data for maintenance and troubleshooting. This provides another way that a US company may have access to data.

If a US company has access (formal or informal) to data from Saskatchewan, either directly or through a controlled subsidiary, the US company could be required to furnish the data to a US law enforcement agency.

## How significant is the risk?

For information in British Columbia, the Information and Privacy Commissioner for British Columbia considered this matter in detail and concluded that there was: "...a reasonable possibility of unauthorized disclosure of...personal information pursuant to an extraterritorial US order or national security letter."[4] British Columbia and several other provinces made changes to their laws in attempts to specifically address risks related to the *USA Patriot Act*.[5]

At the same time, others regard the *USA Patriot Act* as presenting less risk. One reason is that US law enforcement agencies have other ways of obtaining information.

> Canadian and US intelligence agencies share vast amounts of information. Mutual assistance treaties allow Canadian authorities to get warrants for US authorities and vice versa. "Arrangements" exist for informal sharing related to targets of mutual interest. Canadian authorities can get information in the US without a warrant and American authorities can get information in Canada without a warrant.[6]

This suggests that "multilateral treaties and bilateral data sharing arrangements are being used by the US law enforcement far more than the Patriot Act."[7]

According to the Treasury Board of Canada Secretariat, "...it would be much more difficult for most foreign governments to target specific personal information that may be held by a company under the terms of a contract with the Canadian government than it would be to request information through an existing bilateral agreement."[8]

---

[4] Information and Privacy Commissioner for British Columbia, p.18.
[5] British Columbia, for example, amended its *Freedom of Information and Protection of Privacy Act* to specify that public bodies ensure that personal information is stored only in Canada and accessed only in Canada, subject to exceptions. Unauthorized disclosure is prohibited and the changes also required notification in the event of a "foreign demand for disclosure."
[6] Fraser, David, (2011).
[7] Information Technology Association of Canada. (March 2010). *Submission to the Third Legislative Review of the Freedom of Information and Protection of Privacy Act*. http://www.leg.bc.ca/cmt/39thparl/session-2/foi/submissions/organizations/Information_Technology_Association_of_Canada.pdf (October 25, 2011).
[8] Treasury Board of Canada Secretariat (2010), p.9.

Nevertheless, the Treasury Board of Canada Secretariat recommended the need for special attention to government contracts to manage the risks related to the *USA Patriot Act*.[9] Just as Canadian legislation may not dissuade a US company from complying with a legal requirement, within the US, to furnish information, a contract may not prevent disclosure. But these are elements in managing the risk of disclosure.

## How can the risk be managed?

We suggest that government agencies consider the following strategies to manage risks related to the *USA Patriot Act* and data managed and stored by third party contractors.

### Assess risks of using third party contractors

Government agencies should identify risks related to the use of third party contractors. This includes risks related to the *USA Patriot Act*. Agencies should analyze the likelihood and potential impact of risks. For more sensitive information, agencies must take greater precautions.

Agencies should also take into account technical protections that are becoming available to reduce risk. For example, even where data is hosted in the US, Canadian agencies may use encryption to restrict service provider access to sensitive data. In this case, as in most cases, it is not possible to eliminate risk, only reduce it. It is important that agencies decide what level of risk they can tolerate.

### Consider risks when selecting third party contractors

Having assessed risks, government agencies should ensure that they consider those risks in making decisions about service providers. Risk should be considered with other selection criteria in selecting vendors. To allow this to happen, government agencies should ensure they communicate the relevant risks to individuals or groups tasked with making selection decisions.

[9] Ibid., p.1.

## Protect contractually against information being divulged under the *USA Patriot Act*

Government agencies should use the language in contracts to limit disclosure of information. Depending on the nature of the data, government agencies may decide to specify that information must be processed and stored in Canada. Contracts should prohibit disclosure or transfer of information to parties (related or not) outside Canada or allowing such parties to have access to information without written permission. And contracts should enable whatever technical protections government agencies decide to implement, such as restricting access to some data through encryption.

## Consider legislative protection

One further way to protect data is through legislation. We have consulted with Saskatchewan's Information and Privacy Commissioner regarding PAC'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."[10]

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 *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.

[10] Office of the Information and Privacy Commissioner, *2007-2008 Annual Report*, p.7.

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.**

## How did ITO manage the risk?

We studied whether ITO had adequate protections in place to prevent the third party contractor for the data centre from sharing information with its parent company where the parent company was subject to the *USA Patriot Act*. We assessed ITO's protections for the period January 1, 2010 to August 31, 2011.

To evaluate ITO's protections, we used the strategies mentioned in the previous section. Management agreed with these strategies.

We found that ITO assessed the risk of using third party contractors. It analyzed risks related to the *USA Patriot Act*, for example by obtaining legal advice. However, ITO did not document its analysis of risk.

2. **We recommend that the Information Technology Office document its analysis of risks related to the *USA Patriot Act*.**

ITO considered risks related to the *USA Patriot Act* when it selected its service provider. For example, ITO specified in the selection process that the infrastructure was to be located in Saskatchewan.

ITO also built into its contract with the third party contractor provisions specifically designed to manage risks related to the *USA Patriot Act*. ITO specified that specific data (i.e., personal information and personal health information) as well as infrastructure were to remain in Canada. The contract also specified that both ITO and the contractor are responsible for complying with privacy laws.

The protections put in place by ITO cannot ensure that its service provider—the third party contractor—will not share information with the parent company subject to the *USA Patriot Act*. But, as noted, short of a decision to exclude the service provider because of its corporate ownership, the protections in the contract represent a reasonable attempt to manage the risks.

However, as we have described earlier in this chapter, our audit of ITO describes weaknesses that put government information at risk (see Chapter 16 – Information Technology Office). The ITO needs to monitor whether the security requirements the service provider is to follow—including requirements related to the *USA Patriot Act*—are being met. Until it does so, the contractual protections may not be effective in achieving their intended purpose.

## Do other government agencies have information that could be similarly accessed?

Many Saskatchewan government agencies have data that might be accessible through application of the *USA Patriot Act*. This includes agencies using data housed in the US and vendors (US or with US parents) providing maintenance that requires access to data.

ITO manages many IT contracts on behalf of ministries. As described above, ITO includes language in its contracts intended to manage these risks. Crown Investments Corporation of Saskatchewan (CIC) Crown corporations have also considered risks relating to the *USA Patriot Act.* For example, CIC considered the *USA Patriot Act* in formulating policies for CIC Crown corporations and in recommending language for contracts.

We encourage all government agencies to consider the risks related to the operation of the *USA Patriot Act* when making decisions about contracting for IT-related work.

## Glossary

**Cloud computing**—The provision of computer resources as a service over the Internet. The user pays for the amount of service required.

**Data centre**—A central location for computer network hardware and software, especially storage devices for data.

**Encryption**—A method of putting information in code so that only authorized users will be able to see or use the information.

**Network**—A group of computers that communicate with each other.

**Server**—A computer that hosts systems or data for use by other computers on a network.

## Selected references

Canadian Bar Association, BC Branch, Freedom of Information and Privacy Law Section. (2010). *Submission to the Third Legislative Review of the Freedom of Information and Protection of Privacy Act*. http://www.leg.bc.ca/cmt/39thparl/session-2/foi/submissions/organizations/Canadian_Bar_Association%E2%80%93BC_Branch.pdf (October 25, 2011)

Fraser, David. (2011). "Privacy and cloud computing." Presentation October 14, 2011. http://blog.privacylawyer.ca/2011/10/cloudlaw-law-and-policy-in-cloud.html (October 23, 2011)

Fraser, David. (2010). "Patriot Act reality check and Canadian authorities' similar powers." Presentation April 26, 2010. http://blog.privacylawyer.ca/2010/04/patriot-act-reality-check-and-canadian.html (October 23, 2011)

Information & Privacy Commissioner for British Columbia. (2004). Privacy and the USA Patriot Act—Implications for British Columbia Outsourcing [excerpt]. http://www.oipc.bc.ca/images/stories/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final%20summary.pdf (October 25, 2011)

Saskatchewan Information and Privacy Commissioner. (2005). *2004-2005 Annual Report*. Regina: Author. (http://www.oipc.sk.ca/Reports/AnnualReport04-05.pdf) (October 25, 2011)

Treasury Board of Canada Secretariat. (2010). *Guidance document: Taking privacy into account before making contracting decisions.* http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp00-eng.asp (October 25, 2011)

Treasury Board of Canada Secretariat. (2006). *Privacy matters: The Federal strategy to address concerns about the* USA Patriot Act *and transborder data flows.* http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp01-eng.asp (October 25, 2011)