Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

June 16, 2014

Updated guidance on the storage of information outside of Canada by public bodies

B.C.'s *Freedom of Information and Protection of Privacy Act* (FIPPA) prohibits public bodies from storing personal information outside of Canada or allowing access to it from outside of our national border, with specific and limited exceptions. Innovations such as cloud computing have given public bodies pause to consider how these technologies can be used while also respecting the legal restrictions on trans-border flows of personal information.

A recent development in this area is tokenization. Tokenization involves replacing information in an electronic record with a randomly-generated token. The original information can only be linked to the token by what is known as a 'crosswalk table'. Tokenization is distinct from encryption; while encryption may be deciphered given sufficient computer analysis, tokens cannot be decoded without access to the crosswalk table.

Numerous public bodies have sought clarification from this office as to whether the use of tokenization complies with FIPPA, specifically whether tokens can be stored and/or accessed from outside Canada in a manner that complies with the restrictions in section 30.1 of FIPPA.

Public bodies may comply with FIPPA provided that the personal information is adequately tokenized and the crosswalk table is secured in Canada. This includes ensuring that the crosswalk table stored in Canada is not subject to disclosure under U.S. law including the *PATRIOT Act* (or other foreign law instruments).

The OIPC recently provided detailed advice to the BC Government regarding tokenization as it applies to a specific proposed program. Given the considerable interest in this topic by ministries and the broader public sector, we have decided to make this letter a matter of public record. We encourage all public bodies considering the use of tokenization to review this guidance and apply the principles to their specific application.

This office will, in the near future, issue a broadly applicable directive on the application of FIPPA to the privacy challenges represented by this technology.

Office of the
Information &
Privacy Commissioner
for British Columbia
Protecting privacy. Promoting transparency.

April 4, 2014

Bette-Jo Hughes
Associate Deputy Minister
Ministry of Technology, Innovation
and Citizens' Services
PO Box 9412 Stn Prov Govt
Victoria BC V8W 9V1

Nichola Manning
Assistant Deputy Minister
Employment & Labour Market Services Division
Ministry of Social Development and Social Innovation
PO Box 9762 Stn Prov Govt
Victoria BC V8W 1A4

Dear Bette-Jo Hughes and Nichola Manning:

Tokenized data as personal information—OIPC File No. F13-55076

Thank you for the December 13, 2013 briefing on the use of tokenization in relation to the privacy impact assessment ("PIA") for the Ministry of Social Development and Social Innovation's Services to Adults with Developmental Disabilities ("STADD") program. While we have reviewed the PIA, my Office requires more information before we can complete our final analysis of that project. My detailed comments that are specific to the STADD PIA will follow under separate cover once we have received the outstanding information and that review is complete.

However, I understand that government is interested in my comments with respect to the general use and application of tokenization when storing information outside of Canada. To that end I am able to provide the following general comments. It is important to note that these comments are based on documents provided by government in relation to the proposed use of tokenization in the STADD PIA and subsequent representations made to my Office by the Office of the Chief Information Officer.

BACKGROUND

The STADD program is aimed at delivering integrated supports and services to people with developmental disabilities. To accomplish this, the Ministry is developing an integrated network support model that provides a common assessment platform with an online collaborative planning space to support the broad range of professionals who interact with and support individuals with developmental disabilities.

As part of the STADD project, the Ministry proposes to use tokenization as a means to remain in compliance with s. 30.1 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") while storing information outside of Canada. Section 30.1 provides that a public body such as a ministry "must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada". FIPPA defines personal information as "recorded information about an identifiable individual".

Tokenization is a process whereby information in a record is replaced by a randomly-generated token and the token acts as a placeholder for the information in the stored record. A token generally consists of a randomly-generated value (whether alphabetical, numerical, symbol or other value). A log of the replaced information is maintained that links the information to the token. This log, or 'crosswalk table', is used to replace the token with the original information in order to access that information.

The tokenization scheme proposed by government would replace all information that has the potential to identify an individual with one or more tokens before the information is stored outside of Canada. The tokenized information would be stored on servers maintained by Salesforce.com in the United States. The crosswalk table would be stored within Canada on government servers running CipherCloud software, which will manage the crosswalk table. When government employees seek to access tokenized information on foreign servers, the information will be accessed through CipherCloud software, which will de-tokenize the information.

We have been assured by government that CipherCloud and Salesforce.com employees will not have access to any of the information held on government servers or those of its service providers, nor will they have remote access to the software for support purposes. CipherCloud may be provided with software log files in order to facilitate a request for software support, but those logs will not contain any personal information.

Tokenization is distinct from encryption in that while it is technically possible to decipher encrypted information given the use of sufficient computing power, tokenized information cannot be deciphered without the possession of the crosswalk table. This is a significant difference because an individual that is in possession of encrypted information is capable of reverse-engineering the encryption algorithm and accessing the information. Therefore personal information that is encrypted does not lose its character as personal information because it may be re-identified. However, tokenized information cannot be reverse engineered and re-identified because the process of substituting tokens for information is entirely random.

TOKENIZED INFORMATION AND PERSONAL INFORMATION

Because the government does not consider tokenized information to be personal information, it takes the position that tokenized information may be stored outside of Canada without contravening s. 30.1. The Ministry has asked for my comments on this issue. Based on the information that government has provided to my Office, it appears to me that tokenized information is not personal information if the following two key assumptions are met:

1. The information stored outside of Canada is adequately tokenized such that it is not re-identifiable without use of the crosswalk table; and

2. The crosswalk table is stored in Canada and is not accessible outside of Canada.

If these two requirements are met, tokenized information is not personal information because it is not about "an identifiable individual" while in its tokenized form. My Office has previously held that information is "about an identifiable individual" if the information can be linked to an individual through other available information.[1] Other Canadian privacy commissioners, and the courts, have interpreted this language in the same manner.[2] The Ontario Court of Appeal and the Federal Court of Appeal have affirmed the following test regarding whether information is personal information because it is linkable:

> The test then for whether a record can give personal information asks if there is a reasonable expectation that, when the information in it is combined with information from sources otherwise available, the individual can be identified.[3]

My Office has applied that test in several orders and investigation reports.[4] The question therefore is whether tokenized information may be reasonably expected to identify an individual where the tokenized information could only be re-identified using the crosswalk table, which is controlled exclusively by government, within Canada.

Even though the test for determining whether information is personal information is always the same, the kind of activity in question is an important consideration. The perspective from which it is determined whether the information is identifiable depends on the nature of the activity. For this reason, my Office has taken the point of view of

---

[1] Investigation Report F12-04, [2012] B.C.I.P.C.D. No. 23; Order 04-06, [2004] B.C.I.P.C.D. No. 06; and Order P12-01, [2012] B.C.I.P.C.D. No. 25.

[2] See, for example, *Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner)*, 2001 CanLII 32755 (ON SCDC), [aff'd *Ontario (Attorney General) v. Pascoe*, 2002 CanLII 30891 (ON CA)]. The court held in that case that any information which, when combined with other information, could identify a person, qualified as information about an identifiable individual. Also see *University of Alberta v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 112.

[3] *Ontario (Attorney General) v. Pascoe*, 2001 CanLII 32755 (ON SCDC), at para 15, and *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, [2007] 1 FCR 203.

[4] Investigation Report F12-04, [2012] B.C.I.P.C.D. No. 23; Order P12-01, [2012] B.C.I.P.C.D. No. 25; Order F13-04, [2013] B.C.I.P.C.D. No. 4.

the public body when considering whether the public body is collecting or using information about an identifiable individual.[5] In cases involving requests for access to information, however, my Office has taken the point of view of an outsider when considering whether the requested information is about an identifiable individual.[6]

The purpose of s. 30.1 is to protect against third party disclosure, in particular, disclosure to foreign governments and their agencies. Therefore, in my opinion the appropriate point of view in evaluating compliance with s. 30.1 is that of a third party. In this light, the question in relation to tokenization is whether anyone outside the Ministry who gained access to the tokenized information would be accessing information about "an identifiable individual". Based on the information provided, while tokenized information is certainly identifiable to government (which has the crosswalk table), it is not identifiable to anyone outside of government. On this basis, there is not a reasonable expectation that a record containing entirely tokenized information could be considered identifiable by a third party, meaning that tokenized information itself is not personal information as defined in FIPPA.

Again, this view is based on the two assumptions cited above, namely that: the information stored outside of Canada is adequately tokenized such that it is not re-identifiable on its own; and the crosswalk table, even when stored in Canada, is not accessible to third parties outside of Canada. I will now address each of these issues.

RE-IDENTIFICATION OF PARTIALLY TOKENIZED RECORDS

In the case of the STADD program, the Ministry does not intend to tokenize all the information that will be stored outside of Canada. Rather, it intends to tokenize what it believes is a sufficient portion to ensure that the individuals the information is about cannot be identified. Where government chooses to only partially tokenize records stored outside of Canada, the un-tokenized information must be analyzed in advance to ensure that it is not capable of re-identification. While the un-tokenized information itself may not be sufficient to enable identification, it is possible that, depending on the nature of the information, indirect identifiers may be combined such that the individual that the information is about may be identified.

In our review of the STADD program, my Office has raised concerns that the information that is proposed to be left un-tokenized and stored outside of Canada, may be re-identifiable and linked to an individual. This concern would extend to each program that makes use of government's proposed tokenization scheme; government must ensure that it is not storing re-identifiable information outside of Canada. We have committed to work with ministry staff and an expert in re-identification (Dr. Khaled El Emam) to review these specific concerns.

---

[5] Order F13-04, [2013] B.C.I.P.C.D. No. 4.
[6] Order F09-21, [2009] B.C.I.P.C.D. No. 27.

EXTRA-TERRITORIAL REACH OF FOREIGN LAW

The proposed deployment of tokenization by government will provide for the crosswalk table to be stored within Canada. However, in order for the tokenized information that is stored outside of Canada to be considered non-identifying, it is essential that the crosswalk table not be accessible to third parties outside of Canada.

As noted earlier, the intent of s. 30.1 is to address access to personal information by foreign governments and their agencies. As this Office's 2004 report[7] on the topic demonstrated, personal information stored in Canada may be accessed by foreign governments where a company that has custody or control of the personal information is a subsidiary of a foreign company or otherwise amenable to the jurisdiction of a foreign court. A foreign court or government that is authorized by legislation or a rule of court may order a company that is subject to its jurisdiction to produce records even where the information is located in a different country. This principle could in theory apply to enable access to the crosswalk table itself.

There are numerous examples going back decades where American courts have ordered the production of records by American companies where those records are held by foreign subsidiaries.[8] Any company or agency that is within the reach of American legal processes and that has effective access to the requested information can be compelled by American law to provide such information. It is also conceivable that a foreign agency such as the United States Federal Bureau of Investigation could compel a company to produce records where the information relates to criminal or national security matters, and the company has access to the information being sought. The test in these instances is whether the American company has practical control of or a legal right to obtain the records.[9]

Considerations in making this determination include:

- whether there is an intermingling of directors, officers, or employees between the parent and the subsidiary;
- the ability of the parent to direct the appointment of the subsidiary's directors, either directly or indirectly through another corporation or series of corporations;
- the ability of the parent to control the directors of the subsidiary;

---

[7] Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing, October 2004.

[8] *International Shoe v. Washington*, 326 U.S. 310 (1945); *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 131 S. Ct. 2846 (2011); *Re Uranium Antitrust Litigation*, 480 F. Supp. 1138, 1148 (N.D. Ill. 1979); and *First National City Bank of New York v. IRS*, 271 F.2d 616 (2d Cir. 1959).

[9] *Searock v. Stripling*, 736 F.2d 650, 653 (11th Cir. 1984); *In re Folding Carton Antitrust Litigation*, 76 F.R.D. 420, 423 (N.D. Ill. 1977); and *C. Wright & A. Miller*, 8 Federal Practice & Procedure 2210.

- common ownership or the ability to otherwise exercise control over the subsidiary; and

- whether the subsidiary is incorporated in the United States or has continuous and systematic contact with the United States.

Generally, whether a foreign company could be compelled to provide access to a record will depend upon the actual ability of the company to obtain the information. While it is likely that a foreign court will balance the interests of both states where a Canadian statute such as FIPPA would preclude disclosure, it is also likely that foreign interests will outweigh Canadian interests where national security or public safety are said to be at issue.

A key factor in my comments regarding tokenization and compliance with s. 30.1 of FIPPA is the need to protect the crosswalk table from unauthorized access. Because any information breach that involved the crosswalk table would have far-reaching implications, it is important that the security measures in place to protect that file recognize its sensitivity. Government should also have a plan to manage such a breach that addresses the implications for any tokenized information that is stored outside of Canada.

It is the responsibility of government to ensure that these concerns are adequately addressed such that British Columbians can be assured that tokenized information stored outside of Canada cannot be linked to an identifiable individual.

While this letter discusses the implications of government's proposed use of tokenization generally, it does not provide an opinion on any specific program or activity. Its contents will not bind me with respect to any specific matter that may come before me, including any complaint or investigation.

Sincerely,

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

pc: Ian Bailey
Assistant Deputy Minister
Ministry of Technology, Innovation and Citizens' Services