6.2 – Law and Policy

6.2.1 Privacy

Background:

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) governs the management of information and records in the custody or under the control of a public body. "Public body" is defined broadly within FOIPPA to include government ministries, the regulating bodies of professional practices, health authorities, hospitals, post-secondary institutions and school districts, among many more. There are over 3000 public bodies in total in BC.

BC's FOIPPA is widely seen as the most robust privacy regime in Canada, particularly because of its provisions respecting data sovereignty. Shortly after the American Patriot Act was enacted, and growing concerns were raised in BC about outsourcing of government contracts to foreign entities - particularly those in jurisdictions with legislation similar in scope and function to the Patriot Act - BC passed amendments to FOIPPA that would restrict cross-border data flow.

Sections 30 and 33 of FOIPPA in particular are the cause of most difficulties in arranging cross-border data flows, or out of country storage. Section 30 limits the storage of, and access to personal information in the custody or control of a BC public body, and section 33 limits the disclosure of personal information outside of Canada.

What is important to note about how FOIPPA works is that any service provider or contractor is considered to be an employee of the public body contracting them. This means that, as an "employee" of the public body, all of the rules and restrictions of FOIPPA apply to public body service providers in the same way that it applies to any other public body employee. In this way, service providers are not able to do anything that the public body would not be able to do under the law.

Barriers

Storage and Access

Section 30 of FOIPPA, which governs storage of and access to personal information, restricts a public body from storing, or accessing personal information outside of Canada, unless one of three exceptions apply. This means that a public body cannot maintain servers, back up information, upload data to cloud applications or otherwise store personal information outside of the country without a legislative authority. Similarly, a public body cannot provide access to

their systems, permit contractors to access databases, or maintain employees outside of the country if it requires access to personal information without a legislative authority.

The three exceptions that would permit the storage of or access to personal information outside of Canada are [paraphrased]:

(a) with consent, in the prescribed manner;
(b) if the information can be disclosed outside of Canada under s.33.1;
(c) if the information has been disclosed for the purposes of payments made to or by the government of BC (and other administrative functions related to payment).

Given that consent, as a vehicle for compliance is available as a disclosure authority (though different than a consent to store information outside of Canada), and disclosures for the purposes of payments made to or by the government of BC is also an authority for disclosure outside of Canada under section 33.1, the discussion regarding available avenues to a foreign-hosted cloud storage solution is best held in respect to exception (b) above, which permits storage if it is for the purposes of a disclosure authorized under section 33.1. To put it more simply: exceptions (a) and (c) are a subset of exception (b). If a public body is legislatively authorized to disclose personal information outside of Canada, they will also be authorized to store or access that information from outside of Canada. As such, section 33.1 warrants discussion.

Disclosure outside of Canada

Section 33.1 of FOIPPA provides the authorities - of which there are 24 - permitting disclosure inside and outside of Canada. This means that personal information is not permitted to be shared, given to, provided access to, or otherwise disclosed to any person, body, or organization outside of Canada without an authority under section 33.1 allowing it.

The various authorities under section 33.1 are generally purpose- and/or person- based. This is to say that the authorities authorize a disclosure for a very specific reason, or to a very specific person/body. For example, 33.1(1)(k) permits disclosure for the purpose of [paraphrased] licensing, registration and verification of motor vehicle drivers and their insurance. Similarly, section 33.1(1)(g) [paraphrased] permits disclosures to the Attorney General or legal counsel for legal advice. The lone exception to this purpose/person disclosure rule is section 33.1(1)(b) which permits disclosure with consent in the prescribed manner.

There is no disclosure authority that speaks generally to the storage of personal information. There is one disclosure provision that permits the backing up of personal information outside of Canada, but this is heavily conditioned. Section 33.1(1)(p) authorizes disclosures specific to maintenance of data systems however, these disclosures must be temporary and in relation to data recovery may only be used after a system failure has occurred. Essentially, this is not a feasible, long-term solution to storage of personal information outside of Canada.

Given the current legislative landscape, the purpose for which information is to be disclosed outside of Canada must be either one of the purposes set out within section 33.1 (e.g. for the purposes of administering payments to or by the province, etc.), or be done with the consent of the individual whose information is being stored outside of Canada.

Reasonable security measures

FOIPPA does not go into great detail on the matter of technical security. The general security requirement is broad but simply stated:

"A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

It is important to note that the security requirements as stated above stand wholly separate from the storage and access provisions of FOIPPA. This is to say that it is not enough that personal information simply rest within Canada, but that it also remain appropriately secured. Security and data location are separate requirements. A more in-depth discussion on security will be in section 6.2.2 below.

Potential Opportunities:

There is a common misconception that FOIPPA explicitly restricts the ability for a BC public body to use foreign hosted servers. This is not strictly accurate given that they may be used if their use falls within the scope of a current disclosure or storage/access provision. There are also other mechanisms within FOIPPA to address emerging needs. S. 13

S. 13

S. 13 The following are a number of available routes forward in the space of foreign hosted servers. Each option carries with it advantages and disadvantages.

Targeted uses of foreign hosted servers

Targeted uses of foreign hosted servers is essentially the status quo option. This is to say that it does not require any changes to be made or any action – it is currently available to public bodies as a road forward. Targeted uses of foreign hosted servers would include using these cloud servers for a strictly defined subset of actions or purposes. For example, under section 33.1(1)(q) a database of photos or videos taken at public events [paraphrased] could be stored outside of Canada. Similarly, the tax roll or public accounts databases (both including personal information), could be posted online, or stored outside of Canada given their legislatively mandated release. Finally, this solution also includes any uses of cloud servers that do not involve any personal information. Any databases, datasets, or information that does not meet the definition of "personal information" under FOIPPA does not fall under the same restrictions.

The status quo option has the benefit of requiring no major action. Communication and training are required to ensure that public body employees are aware of this frequent misconception, and also to ensure that those venturing forward into the cloud space are doing so on sure legal footing and in ways that do not present undue risk. The disadvantage of this route forward is that it does not address those public bodies that would like to use foreign hosted servers and do not have a legislated purpose (i.e. disclosure provisions) that would allow them to do it.

Tokenization

Tokenization is a technical means by which personal information can be removed from a database or application and replaced with an arbitrary value. Tokenization can be configured in such a way that databases or datasets can be placed on foreign applications while the personal information in that database is replaced (and so remains within Canada), sending only non-identifiable information across the border. In this way, the features of a foreign application can be used, while the restrictions of FOIPPA are upheld.

The advantages of this approach are that it is a technical means of using cloud solutions without requiring legislative authority to do so. In this way, the use is not tied to a purpose, meaning that cloud services configured with tokenization can be used for any use that fits the tool or application in question. Further, given that this approach opens the door to using foreign applications, the cost – even while factoring in the cost of tokenization – is potentially much lower than it would be to deliver the same product within Canada.

The disadvantage of this approach is that there is an added cost in order to tokenize information or systems. This results in a cost issue for smaller systems or databases. The added cost of tokenization may only be efficient in places where a high amount of money is being spent anyways (i.e. $1000 tokenization on a $100 system likely does not make financial sense). Additionally, if a lot of fields or items in a database or dataset are being tokenized, it is possible that the system will slow down and not operate as efficiently as it would were there no fields tokenized.

Ministerial order

Section 33.1(3) provides the Minister responsible for FOIPPA the power to allow, by order, disclosures outside of Canada [paraphrased]. The resulting “ministerial order” can put any conditions or restrictions on the disclosure authority, however, as a limitation, this new disclosure authority must be something that would already be authorized under section 33.2 (disclosures inside of Canada only). This is a solution that has been used three times in the past, most recently being used to permit the disclosures that are inherent to citizen engagement in the social media realm. S. 13

S. 13

As discussed above, with the addition of an authority to disclose outside Canada, the public body is provided a corresponding authority to store that information outside of Canada. Therefore, a ministerial order stands as an available option for providing public bodies the ability to store personal information on foreign hosted servers – as long as an appropriate provision is able to be drafted given the restrictions (i.e. that the basis of the authority already exists under section 33.2).

Given the significance of a ministerial order (namely the scope of its effect), it is likely to involve the Office of the Information and Privacy Commissioner (OIPC), the regulator responsible for overseeing and enforcing FOIPPA. S. 13

S. 13

Any ministerial order, or FOIPPA/ministry specific amendment that permitted general, broad in scope disclosures of personal information outside of Canada could also be seen as a total override of the storage, access and disclosure provisions of FOIPPA. The ability to store any personal information outside of Canada would essentially allow for all of government's personal information to be stored outside of Canada, thereby negating the usefulness and effectiveness of these provisions S. 13

S. 13

S. 13 For this reason, any ministerial order or FOIPPA/ministry specific amendments would have to be limited and narrow in scope – which naturally limits their usefulness in the context of foreign hosted storage of data.

S. 13

Page 6 redacted for the following reason:
- -
S. 13