Discuss the current state of data residency (i.e. data localization) requirements in BC, and provide your opinion about whether there should be data residency requirements. If not, explain why not. If so, explain the extent of the requirements that are desirable to have in law.

Data Residency Requirements for Public Bodies in British Columbia

Name: Manveer Sall
Date: December 3, 2021
Law 343 A02

Introduction

The evolution of the internet and cloud-based services has created new avenues for communication, learning, data storage, and information exchange. Simultaneously, however, this evolution has raised new challenges for governments to find ways to protect the personal information of its residents. Governments around the world have responded to these new challenges by implementing "data residency" requirements meant to safeguard the public from having their personal information accessed by foreign entities. Data residency is achieved when personal information is stored and accessed within a country's own border.[1]

The data residency requirements for public bodies in BC are outlined in the *Freedom of Information and Protection of Privacy Act ("FIPPA").* Under *FIPPA,* a public body includes a ministry of the government of BC or local public bodies, such as the ones found in health care, education and social services.[2] As such, the data residency requirements for public bodies in *FIPPA* apply to a vast array of public entities that hold some of the most sensitive personal information belonging to British Columbians.

Following a discussion about the current state of data residency requirements in BC, this paper will argue that BC should retain a robust, yet versatile, data residency regime. Specifically, BC's data residency requirements should follow a risk-based approach that allows public bodies to weigh the benefits of using third-party tools and applications against the risk of potentially exposing personal information to foreign actors.

This paper will begin with a discussion of the current state of data residency requirements in BC, including the law as it stands today, the temporary Covid-19 exemptions, and the recently proposed legislative changes to the requirements. Part II will outline some of the pros and cons

[1]Cloud Privacy Working Group, *Privacy and Cloud: Guidance for MPOs* (2019), at 2 [*Guidance for MPOs].*
[2] *Freedom of Information and Protection of Privacy Act,* RSBC 1996, Chapter 165, at Schedule 1 [*FIPPA]*.

of data residency laws, as a means to illustrate why BC should retain a degree of data residency requirements. Finally, Part III will describe what a modernized risk-based approach to data residency might entail.

Part I: Current State of Data Residency Requirements in BC

Data residency requirements in BC are currently in a state of flux. On one hand, the data residency requirements in *FIPPA* are still technically in effect. On the other hand, a number of temporary exemptions have been implemented through a series of Ministerial Orders as a response to the Covid-19 pandemic. To add further uncertainty to the data residency landscape in BC, Bill 22, also known as the *Freedom of Information and Protection of Privacy Amendment Act*, has proposed a new, more relaxed, data residency regime for the future.

FIPPA Section 30.1 and 33.1

Section 30.1 and 33.1 provide a good starting point for the discussion on the current state of data residency requirements in BC. Section 30.1 is reproduced below:

Storage and access must be in Canada

> **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).[3]

[3] *FIPPA, supra* at note 2, s 30.1.

Section 30.1 stipulates that public bodies must store and access personal information in its custody or control only in Canada. For example, if a local educational body such as Surrey School District 36 is using a cloud service to store personal information of its students, the cloud service must have its data centers in Canada. Moreover, the data centers should be architected such that personal information remains in Canada throughout the data storage process.[4]

There are a few general exceptions to the s. 30.1 requirement that are enumerated in subsection (a) through (c). For instance, s. 30.1(a) allows public bodies to store personal information outside of Canada with the informed consent of the individual to whom the personal information belongs. However, seeing as public bodies generally have control over personal information belonging to many individuals, this exception is not far-reaching in practice. For instance, it would not be practical for a health body to seek consent from each and every patient to store their health data in data centers located outside Canada.

Further exceptions are provided in s. 33.1 of *FIPPA*, two of which are reproduced below:

Disclosure inside or outside Canada

33.1 (1)A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

(f)to an officer or employee of the public body or to a minister, if the information is immediately necessary for the protection of the health or safety of the officer, employee or minister

…

(p)if the disclosure

(i)is necessary for

[4] *Guidance for MPOs, supra* note 1 at 2.

(A)installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or equipment that includes an electronic system, or

(B)data recovery that is being undertaken following the failure of an electronic system

that is used in Canada, by the public body or by a service provider for the purposes of providing services to a public body, and

(ii)in the case of disclosure outside Canada, results in temporary access and storage that is limited to the minimum period of time necessary to complete the installation, implementation, maintenance, repair, troubleshooting, upgrading or data recovery referred to in subparagraph (i);[5]

The above reproduction of two of the s. 33.1 subsections is not meant to be exhaustive, as there are more than a dozen exceptions. However, the reproduction is meant to illustrate the narrow scope of the exceptions available to public bodies to store and access data outside of Canada. Many of the exceptions in s. 33.1 address specific circumstances in which personal information can be disclosed outside of Canada only when necessary.

For example, ss. 33.1(e) allows disclosure outside of Canada if a minister, officer, or employee of a public body needs the information to perform their duties while outside of Canada on a temporary basis.[6] Subsection 33.1(f) allows officers or employees of a public body to access data outside of Canada when it is necessary for the protection of their health or safety.[7]

[5] *FIPPA, supra* at note 2, s 33.1 (f) and (p).
[6] *FIPPA, supra* at note 2, s 33.1(e).
[7] *FIPPA, supra* at note 2, s 33.1(f).

Subsection 33.1(p) allows disclosure outside of Canada for the purpose of conducting maintenance or repair work to services otherwise resident in Canada.[8] This exception is a temporary one that is only meant to cover the time period required to complete the necessary work on the system.

Taken together, s. 30.1 and s. 33.1 of *FIPPA* impose strict data residency requirements for public bodies in BC. Generally, public bodies must not disclose personal information outside of Canada. Although certain exceptions are provided in both s. 30.1 and s. 33.1, they only apply in very specific circumstances and often to only a select class of individuals, such as ministers or officers of public bodies.

Covid-19 Exemptions

It would be inaccurate to discuss the current state of data residency requirements in BC without mentioning the temporary exemptions currently in place. On March 26, 2020, the government of British Columbia issued Ministerial Order No. M085. The recitals in the Order stated that the temporary provisions were enacted to facilitate "efficient and prompt collaboration and communication [as] required to protect the health, safety and welfare of the residents of British Columba during the Covid-19 pandemic.[9]

For health care bodies, the Order stipulated that:

> 1. A health care body as defined in the Freedom of Information and Protection of Privacy Act, or the Ministry of Health, the Ministry of Mental Health and Addictions, or the Provincial Health Services Authority may disclose personal information inside or outside of Canada in accordance with s. 33.2(a) and (c) of the Freedom of Information and Protection of Privacy Act on the condition that the disclosure is necessary:
>
> > a. for the purposes of communicating with individuals respecting COVID-19,

[8] *FIPPA, supra* at note 2, s.33.1 (p).
[9] Ministerial Order M085, (2020)

> b. for the purposes of supporting a public health response to the COVID-19 pandemic, or
>
> c. for the purposes of coordinating care during the COVID-19 pandemic.[10]

For public bodies other than health care bodies, such as educational bodies, the Order held that:

> 2. A public body may disclose personal information inside or outside of Canada in accordance with s. 33.2(a) or (c) of Freedom of Information and Protection of Privacy Act through the use of third-party tools and applications on the condition that the disclosure is for the following purposes:
>
> > a. the third-party tools or applications are being used to support and maintain the operation of programs or activities of the public body or public bodies,
> >
> > b. the third-party tools or applications support public health recommendations or requirements related to minimizing transmission of COVID-19 (e.g. social distancing, working from home, etc.), and
> >
> > c. any disclosure of personal information is limited to the minimum amount reasonably necessary for the performance of duties by an employee, officer or minister of the public body.[11]

The net effect of these provisions was to grant public bodies a degree of flexibility when responding to the pandemic. For instance, in an emailed statement by the Ministry of Citizens' Services, a spokesperson gave an example of how someone who was self-isolating may only know how to use one specific phone application to communicate with a nurse.[12] Without the Covid-19 data residency exemptions, the nurse would not be able to communicate with the patient if the application being used stored data outside of Canada. With the temporary exemptions, however, the nurse could go ahead and administer health aid without having to first

---

[10] *Ibid.*
[11] *Ibid.*
[12] Brenna Owen, "B.C. temporarily lifts requirement on storing personal data in Canada due to COVID-19", *CTV News* (4 April 2020), online: < https://bc.ctvnews.ca/b-c-temporarily-lifts-requirement-on-storing-personal-data-in-canada-due-to-covid-19-1.4882836> [*CTV News Article].*

embark on a technological quest to find a suitable phone application with the patient. Another benefit of the temporary Covid-19 exemptions was to support the abrupt transition to teleworking for many public bodies by allowing the use of third-party applications that may otherwise be restricted due to data residency requirements.

Since the temporary Covid-19 exemptions stray quite far from the otherwise strict data residency requirements on public bodies in BC, the Ministerial Order included language to provide some protection for personal information. The Order had the following provision:

> 3. A public body must not disclose information under sections 1 or 2 unless the head of the public body is satisfied that with respect to the information disclosed:
>
> > a. the third-party application is reasonably secure in compliance with s. 30 of the Freedom of Information and Protection of Privacy Act; and
> >
> > b. the public body makes all reasonable efforts to remove personal information which is collected, used or disclosed using a third-party application from the third-party application as soon as is operationally reasonable and the public body retains and manages the information, as required by law.[13]

The practical effect of section 3 seems to be that public bodies must still exercise caution when selecting third-party applications. Aside from subsection (a) ensuring that the applications are reasonably secure, subsection (b) goes a step further by reiterating the temporary purpose of the Covid-19 exemptions. The Ministry of Citizens' Services provided an example where if a health care team set up a Slack channel to communicate, they would have to delete any personal information shared on the application as soon it was operationally reasonable to do so.[14]

The temporary Covid-19 exemptions have been in place since the initial order in March 2020. At first, the Order was to stay in effect until June 30, 2020. However, a series of

[13] Ministerial Order M085, (2020)
[14] *CTV News Article, supra* at note 11.

subsequent Ministerial Orders have renewed the temporary exemptions until December 31, 2021.[15]

Bill 22: *Freedom of Information and Protection of Privacy Amendment Act*

As of writing this paper, the majority NDP government in BC passed Bill 22 in the legislature.[16] Bill 22 makes several major changes to the information and privacy regime in the province, including to the data residency requirements for public bodies. Most notably, s. 30.1, which is reproduced on page 2 above, has been repealed. Recall that s. 30.1 prohibited public bodies from storing or accessing personal information in its control or custody outside of Canada.[17] In addition to repealing s. 30.1, Bill 22 has added a new s. 33.1 that states that a "public body may disclose personal information outside of Canada only if the disclosure is in accordance with the regulations, if any, made by the minster responsible for this Act." [18]

Bill 22 has major ramifications on the data residency regime for public bodies as it has seemingly opened the door to store and access data outside of Canada, provided that it is not against the regulations to do. However, the government has not provided any insights into what potential regulations could look like, or whether any regulations will even be made. In fact, the new s. 33.1 explicitly leaves the door open for this latter possibility by including "if any" in reference to potential future regulations.

Bill 22 has been met with a great deal of opposition from various parties. For example, Michael McEvoy, the Information and Privacy Commissioner for British Columbia, released a statement that is very critical of the new data residency regime. Commissioner McEvoy states

---

[15] Ministerial Order M192, (2021)

[16] Bhinder Sajan, "B.C. NDP passes controversial FOI bill that may mean fees for public information requests, *CTV News* (25 November 2021), online: < https://bc.ctvnews.ca/b-c-ndp-passes-controversial-foi-bill-that-may-mean-fees-for-public-information-requests-1.5682119>.

[17] *FIPPA, supra* at note 2, s 30.1.

[18] *Freedom of Information and Protection of Privacy Amendment Act 2021,* s 33.1

"An overriding concern with Bill 22 is the unknown impact of key amendments because their substance will only be filled in through regulations, about which we know nothing".[19] The commissioner goes on to say that it is, "crucial for the government to disclose now what it intends to do to protect the personal privacy of British Columbians whose personal information may be exported outside Canada".[20]

It appears that data residency requirements in BC, specifically as they pertain to public bodies, have followed a linear trajectory from strict to relaxed regulations. The current data residency requirements in s. 30.1 and 33.1 are illustrative of a strict data residency regime that prioritizes the safety of personal information over all else. With the onset of the Covid-19 pandemic, the provincial government took a more pragmatic approach by loosening its data residency requirements. This was done to provide leeway for public bodies to efficiently respond to the emerging needs of the pandemic. Almost twenty months after the temporary exemptions were first implemented, Bill 22 has now effectively removed all data residency requirements for public bodies, since there are no restricting regulations passed at the time of this writing.

Part II: A Case for Retaining Data Residency Requirements for Public Bodies in BC

With the dramatic rise of the internet and online applications, individuals have become increasingly alarmed about the collection and use of their personal information.[21] As Chen-Hung Chang argues, whereas traditional notions of information privacy centered around personal control over data about oneself, emerging technologies have rendered it nearly impossible for

[19] Office of the Information and Privacy Commissioner for British Columbia, *Re: Bill 22- Freedom of Information and Protection of Privacy Act amendments,* 2021, by Michael McEvoy, at 1.
[20] *ibid*
[21] Craig D. Tindall, "Argus Rules: The Commercialization of Personal Information" [2003] 2003:1 U III JL Tech & Policy 181, at 182 [*Tindall].*

individuals to protect their personal information without outside help.[22] To further complicate matters, when it comes to public bodies, individuals may not have a choice about whether to engage with the technologies and third-party applications used by any given public body. For example, "Kahoot!" is an educational tool commonly used in schools. According to their privacy policy, "[Kahoot] collect[s] information globally and may transfer, process, and store your information outside of your country of residence".[23] Imagine a scenario where a sixth-grade student is asked by their teacher to participate in a Kahoot exercise. Regardless about how the student, or the student's parents, feel about sharing personal information, they likely would conform to the exercise to avoid any hinderances to the student's learning. As such, even those who choose not to use the internet, smartphones, and social media on their own accord, may nevertheless find themselves "trapped in the inescapable digital net" when they interact with public bodies.[24]

Government Accountability

To counteract the lack of choice that individuals may have when dealing with public bodies, data residency requirements place some power back in the hands of individuals in the form of government accountability. If data is stored within Canada and the public feels that the data centers are not adequately protected, they can use their democratic rights to advocate for change. The power to influence change is especially strong in Canada since it is often ranked in the 90-100th percentile of the Voice and Accountability World Index.[25] This index captures the extent to which a country's citizens are able to participate in selecting their government, as well

[22] Chen-Hung Chang, "New Technology, New Information Privacy: Social-Value-Orientated Information Privacy Theory" (2015) 10:1 NTU L Rev 127, at 131 [*Chang]*.
[23] Kahoot! Privacy Policy (28 July 2021), online < https://trust.kahoot.com/privacy-policy/>
[24] *Chang, supra* at note 21, at 127.
[25] World Bank, "Worldwide Governance Indicators" (2010), online < https://info.worldbank.org/governance/wgi/Home/Reports>

as freedom of expression, association, and media. In other words, British Columbians wield actual power to influence how their data is stored and protected within Canada in the event that they are unhappy with how their personal information is being handled. Without data residency requirements, the public loses proximity, and therefore visibility, of their personal information which can hinder their knowledge about how their personal information is being handled.

The element of "proximity" or "visibility" can help provide individuals with a degree of control over their personal information as opposed to having their data shipped across the world to an unknown country. The rationale behind this "proximity" or "visibility" argument is not new, however it has mostly been applied from the government's perspective. For instance, Cohen et al. notes that "some [countries] require as a matter of national security the local storage or processing of data by government contractors or data related to critical infrastructure such as power plants".[26] Aside from interference from foreign actors, the motivation behind storing critical information locally is the ability to exercise greater control over its storage and protection. A similar argument can be made from the public's perspective. Critical information, such as sensitive data related to health or finances, should be stored locally so that the public has greater control and visibility over their personal information.

Foreign Interference

Data residency requirements for public bodies are necessary to protect sensitive personal information from foreign state actors. In the privacy sphere, it is accepted that some governments implement data residency requirements due to the increased surveillance of global data by foreign intelligence agencies.[27] In the post 9-11 world, the United States led the charge to

[26] Bret Cohen, Britanie Hall, and Charlie Wood, "Data Localization Laws and their Impact on Privacy, Data Security and the Global Economy" (2017) 32:! Antitrust 107, at 107 [*Cohen, Hall, & Wood].*
[27]*Cohen, Hall, & Wood, supra* at 108.

aggressively increase their foreign data surveillance as a means to counter terrorism. As Stephen Schulhofer notes, the *Patriot Act* has subjected non-US residents to long periods of unregulated monitoring.[28] The individual is typically not even notified that they have been the subject of data surveillance.[29] The net effect of this latter point is that the full extent of foreign data surveillance is unknown, the only thing that is certain is that it is commonplace.

Data surveillance by foreign entities, including governments, was the subject of a Court of Justice of the European Union decision in 2015 called *Schrems v DPC*. In this decision, Judge Hogan declared that it was reasonable to believe that companies, such as Facebook, routinely send personal information belonging to its users back to the United States where it is accessed by the National Security Agency (NSA).[30] Judge Hogan went on to say that the NSA then undertakes mass and indiscriminate surveillance of the data.[31] Unfortunately, most surveillance a government does outside its own national borders is an "international law free-for-all".[32]

Given the "free-for-all" that exists in the international sphere with respect to foreign intelligence surveillance, it makes sense then for British Columbia to remain vigilant and take steps to preserve the personal information held by public bodies in the province. Implementing data residency requirements is one such step. By encouraging public bodies to store data within Canada, the risk of a foreign governmental entity, such as the NSA, accessing personal information is greatly reduced.

---

[28] Stephen J. Schulhofer , "The New World of Foreign Intelligence Surveillance" (2006) 17:2 Stanford Law & Policy Review 531, at 536 [*Schulhofer].*

[29] *Schulhofer, supra* at note 27, at 534.

[30] Andrea Mulligan, "Constitutional Aspects of International Data Transfer and Mass Surveillance" 55 Irish Jurist (NS) 199, at 202 [*Mulligan*]

[31] *Mulligan*, at 202.

[32] William C. Banks, "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage" (2017), at 518.

Proponents of relaxed data residency requirements may argue that data residency is an ineffective strategy to prevent unauthorized access to personal information because non-governmental organizations are a major source of cyberattacks. In fact, some reports suggest that the majority of cyber-attacks worldwide are launched by non-state actors.[33] However, the simplest counterargument to this is best illustrated by the old adage, "something is better than nothing". For example, if public bodies in British Columbia stored personal information outside of Canada, the potential threats to the data would be two-fold. On one hand, the data would be more easily accessible to the domestic government of whichever country the data is located. On the other hand, the data is still vulnerable to cyber-attacks by non-state actors. In contrast, if public bodies stored personal information within Canada only, the primary threat would only be from non-state actors. The concern over foreign intelligence surveillance is mitigated when data is stored within the Canadian border.

A Case Against Data Residency

A primary argument for removing, or loosening, data residency requirements is that they tend to handcuff public bodies from using online services and applications that would otherwise be useful. In a "Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act", a number of public bodies expressed concerns about how data residency requirements have affected their day-to-day business activities.[34] For example, a number of health bodies issued a joint statement, "describing challenges it [data residency] presents for them, including impairing their ability to use technologies, global expertise, and data services."[35] Similarly, several universities expressed concerns about data residency requirements

[33] Sico van der Meer, "How states could respond to non-state cyber-attacks" (2020) Clingendael Institute, at 1.
[34] *Report of the Special Committee to Review the Freedom if Information and Protection of Privacy Act* (2016), at 28.
[35] *Ibid.*

by identifying, "negative impacts on administrative efficiency and security, international engagement and student recruitment, online learning offerings, and academic integrity".[36] The health bodies and the educational institutions concluded by saying that public bodies should be allowed to store and disclose personal information outside of Canada as long as the risks to privacy are mitigated.[37]

The argument that strict data residency requirements prohibit public bodies from using certain online services that may otherwise improve operational efficiencies is a valid one. For this reason, the remainder of this paper will outline a modernized, risk-based approach, to data residency that can help preserve the many benefits of data residency while simultaneously addressing the concerns of public bodies wishing to use online services and applications that store data outside of Canada.

Part III: A Risk-Based Approach to Data Residency Requirements for Public Bodies in BC

A paramount consideration of any new data residency regime in British Columbia needs to put the protection of personal information at the forefront. To this end, a section similar to s. 30.1 of *FIPPA* should be a staple of any new legislative scheme for data residency. Recall that s. 30.1 of *FIPPA* states that 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".[38] Retaining a provision such as s. 30.1 in the data residency requirements would create a presumption that public bodies store personal information within Canada. However, a broad risk-based exception to the data residency presumption should be available to provide public bodies with flexibility to utilize online services and applications that store data outside of Canada.

---

[36] *Ibid.*
[37] *Ibid.*
[38] *FIPPA*, *supra* at note 2, at s 30.1.

A risk-based exception is one that is centered on "whether there is a significant likelihood that an identified threat could lead to a recognized harm with a significant degree of seriousness."[39] Whereas the current approach to data residency requirements consists of regulators setting strict standards and enforcing compliance in a uniform manner, a risk-based approach to data residency would provide for a more versatile solution.[40] This is because a risk-based approach to data residency would allow public bodies to focus less on bureaucratic requirements that do not necessarily afford better protection of personal information, and instead focus on identifying technology solutions that increase efficiencies while also offering strong data protection mechanisms.

Structure of Risk-Based Approach

The following steps illustrate how the risk-based exception model discussed above would work in practice:

1. There is a presumption that all personal information in the custody or control of public bodies in BC is stored and accessed within Canada only;
2. If a public body wishes to use a third-party application or tool that stores data outside of Canada, they can rely on a risk-based exception to circumvent the general presumption in Step 1;
3. To rely on the risk-based exception, the public body must show that there are compelling reasons as to why the third-party tool or application is a more viable option compared to other similar alternatives that comply with the data residency presumption in Step 1 (this will collectively be referred to as the "threshold requirement"). At this stage, the public

[39] Centre for Information Policy Leadership, "A Risk-based Approach to Privacy: Improving Effectiveness in Practice" (2014), at 4 [*A Risk-based Approach to Privacy].*

[40] Francesca Episcopop, "The Risk-Based Approach to Data Protection Book Reviews" (2021) 7:1 European Data Protection Law Review 143, at 143.

body should make reference to specific alterative tools and applications that are considered possible alternatives;

4. If the threshold requirement is met, the public body needs to do a detailed risk assessment to determine if the benefits of using the third-party tool or application outweigh the potential security risks of disclosing personal information outside of Canada;
5. If the benefits outweigh the potential security risks, the public body can proceed with using the third-party application or tool. Moreover, the third-party tool or application will be added to a central repository of approved third-party tools and applications to be available for use by other public bodies in the future;
6. If a public body wishes to use a third-party tool or application that is available in the central repository mentioned in Step 5, a streamlined risk assessment must be conducted. The purpose of the streamlined risk assessment is to simply verify that all information contained in the original risk assessment is still valid and that no material changes in the privacy policy of the third-party tool or application have occurred.

Factors to Consider during Risk Assessment (Step 4)

There are a number of different factors that can be considered during a risk assessment in Step 4. As mentioned above, the central question during the risk assessment should focus on the significant likelihood that an identified threat could lead to a recognized harm. When analyzing threats, the public body should assess the third-party tool or application to determine if it undertakes unjustifiable or excessive collection of data, inappropriate use of data, and whether data is stored in a secured location where the risk of a data breach is minimal.[41]

[41] *A Risk-based Approach to Privacy, supra* at note 39, at 6.

Additional factors can be borrowed from the European Union's General Data Protection Regulation (GDPR), specifically with respect to the adequacy status provisions. GDPR is considered one of the foremost data protection regimes in the world because it imposes comprehensive obligations on organizations anywhere in the world that are dealing with data related to people in the EU.[42] Adequacy status is one aspect of the GDPR that assigns an indicator to certain countries that have sufficient levels of data protection. The factors considered in the assessment include the country's respect for human rights and fundamental freedoms, privacy legislation in place, the degree of access that public authorities have to personal data, and the existence and effectiveness of an independent supervisory authority for data protection.[43] These factors can be considered by public bodies when assessing the level of risk associated with using a third-party tool or application that stores data outside of Canada.

In addition to the factors listed above, public bodies should consider the service provider's history, specifically with respect to any data breaches or privacy issues. For instance, if the third-party tool or application is produced by a company that has a history of data breaches, this should weigh heavily against using that application. The public body should also assess the service provider's privacy policy to ensure that adequate data protection measures are in place. Furthermore, public bodies should consider whether contractual provisions can be added into the purchase agreement that provide safeguards to personal information. For example, perhaps a term can be added into the purchase agreement that ensures that personal information is only accessed in limited circumstances. Another possible term that can be added is for the service provider to respect a user's right to be deleted. These are just two examples of the kinds of terms that can be added into a purchase agreement to make it more appropriate from a privacy

[42]Ben Wolford, "What is GDPR, the EU's new data protection law?", online: <https://gdpr.eu/what-is-gdpr/>
[43] EC, *General Data Protection Regulations,* Article 45, s 2(a)

protection standpoint. Perhaps public bodies can also get guidance from relevant organizations when they are completing these risk assessments, such as the Office of the Information and Privacy Commissioner for BC.

Taken together, the risk assessment is not meant to be a rigid framework, but rather, it affords public bodies with some flexibility to use their best judgement to make a decision. As the Centre for Information Policy Leadership noted in their work on a risk-based approach to privacy, "risk assessment and risk management call for judgement, based upon honest, well-informed and justifiable answers to structured questions about threats and harms". As such, although a consistent framework should be established, there need not be one uniform method for risk assessment.

Part IV: Conclusion

There is an interesting trichotomy in the current state of data residency requirements for public bodies in British Columbia. As the current requirements in *FIPPA* make way for the new provisions proposed in Bill 22, it appears that BC is going from one extreme, the current strict requirements, to another, being the complete loosening of requirements under the new scheme. In the meantime, a middle ground exists between these two extremes in the form of the temporary Covid-19 data residency requirements.

As this paper illustrates, data residency requirements are crucial to protecting the sensitive personal information of British Columbians. The benefits of storing personal information within Canada include government accountability over the data, protection against foreign intelligence, and easier access by local law enforcement. The main drawback, however, is that data residency requirements can hinder operational efficiency by forcing public bodies to forgo using third-party tools and applications that store data outside of Canada. Fortunately,

implementing a risk-based exception to a general presumption of data residency can provide public bodies with the flexibility to use third-party tools and applications.

Bibliography

Andrea Mulligan, "Constitutional Aspects of International Data Transfer and Mass Surveillance" 55 Irish Jurist (NS) 199.

Ben Wolford, "What is GDPR, the EU's new data protection law?", online: https://gdpr.eu/what-is-gdpr/

Bhinder Sajan, "B.C. NDP passes controversial FOI bill that may mean fees for public information requests, *CTV News* (25 November 2021), online: < https://bc.ctvnews.ca/b-c-ndp-passes-controversial-foi-bill-that-may-mean-fees-for-public-information-requests-1.5682119>.

Brenna Owen, "B.C. temporarily lifts requirement on storing personal data in Canada due to COVID-19", *CTV News* (4 April 2020), online: < https://bc.ctvnews.ca/b-c-temporarily-lifts-requirement-on-storing-personal-data-in-canada-due-to-covid-19-1.4882836>.

Bret Cohen, Britanie Hall, and Charlie Wood, "Data Localization Laws and their Impact on Privacy, Data Security and the Global Economy" (2017) 32:! Antitrust 107.

Cloud Privacy Working Group, *Privacy and Cloud: Guidance for MPOs* (2019).

Centre for Information Policy Leadership, "A Risk-based Approach to Privacy: Improving Effectiveness in Practice" (2014)

Chen-Hung Chang, "New Technology, New Information Privacy: Social-Value-Orientated Information Privacy Theory" (2015) 10:1 NTU L Rev 127.

Kahoot! Privacy Policy (28 July 2021), online < https://trust.kahoot.com/privacy-policy/>.

Craig D. Tindall, "Argus Rules: The Commercialization of Personal Information" [2003] 2003:1 U III JL Tech & Policy 181.

EC, *General Data Protection Regulations,* Article 45, s 2(a).

Francesca Episcopop, "The Risk-Based Approach to Data Protection Book Reviews" (2021) 7:1 European Data Protection Law Review 143

Freedom of Information and Protection of Privacy Act, RSBC 1996, Chapter 165, s 30.1.

Freedom of Information and Protection of Privacy Amendment Act 2021, s 33.1

H Jacqueline Brehmer, "Data Localization: The Unintended Consequences of Privacy Litigation" (2018) 67:3 American University Law Review 927.

Ministerial Order M192, (2021)

Ministerial Order M085, (2020)

Office of the Information and Privacy Commissioner for British Columbia, *Re: Bill 22- Freedom of Information and Protection of Privacy Act amendments,* 2021, by Michael McEvoy. *Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act* (2016)

Sico van der Meer, "How states could respond to non-state cyber-attacks" (2020) Clingendael Institute.

Stephen J. Schulhofer , "The New World of Foreign Intelligence Surveillance" (2006) 17:2 Stanford Law & Policy Review 531.

William C. Banks, "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage" (2017).

World Bank, "Worldwide Governance Indicators" (2010), online < https://info.worldbank.org/governance/wgi/Home/Reports>.