Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

June 9, 2022

Local Law Assessments and Online Services – Refining the Approach to Beneficial and Privacy-Protective Cross-Border Data Flows

A Case Study from British Columbia

I. Executive Summary

Cross-border data flows are critical for the modern digital ecosystem. Without them, public and private sector bodies and individuals will lack access to a wide range of tools and services that are essential to an efficient and safe digital economy and society, including effective cyber security and fraud prevention tools. They are also a key driver of economic growth. The benefits of the free flow of personal data across borders can be put at risk by laws and policies ostensibly premised on data protection objectives that have the effect of localizing data within the jurisdiction of origin. These laws and policies range from direct data localization requirements to various restrictions on data transfers, such as a requirement for organizations to conduct transfer risk assessments, or local law assessments, prior to a transfer. Such assessments focus heavily on the risk that a foreign government may gain inappropriate access to transferred personal data.

Conducting local law assessments for each of the multitude of countries to which data is transferred on a daily and ongoing basis presents a substantial and, in the long run, unsustainable burden for both private and public sector bodies. When this requirement is coupled with an approach that effectively prohibits such transfers if any risk is found that cannot be completely removed through a range of protective measures, no matter how low the risk is and no matter the benefits of the transfers, a local law assessment requirement will have a substantially negative impact on local digital economies and societies that depend on efficient cross-border data flows.

Recent developments in British Columbia signaled a recognition of the importance of cross-border data flows to an efficient and effective public sector. Specifically, the British Columbian public-sector privacy law, the Freedom of Information and Protection of Privacy Act ("FOIPPA"), was recently amended to remove data localization requirements and significant limits on data transfers.[1] However, soon afterward, guidance from the Office of the Information and Privacy Commissioner ("OIPC") appeared to nevertheless require public bodies to conduct local law assessments (or transfer risk assessments) when using cloud services that involve processing or storage of personal data outside of Canada.[2]

To avoid the potential pitfalls of such a requirement and to safeguard the legislative goal of the recent FOIPPA amendments to enable public bodies to use modern digital tools that rely on cross-border data flows, we recommend that the local law assessment requirement found in the OIPC's guidance be clarified to ensure that it can be applied in a risk-based fashion. A risk-based approach to local law assessments avoids any categorical prohibition against transfers (for example, even after appropriate mitigations have been implemented and the benefits substantially outweigh the transfer risk), and also recognizes that local law assessments are not required in all circumstances. Specifically, this paper proposes that (1) a local law assessment should be only one of many potential factors to be considered when transferring personal data outside of a jurisdiction; and (2), a local law assessment should not be required in instances

where the security and privacy controls applied to the data sufficiently mitigate the potential risks of unauthorized access presented by local law, or the transferred data are historically and demonstrably of little interest to foreign governments. Such an approach would both enable public-sector entities to reap the benefits of innovative cloud-based technologies, while also encouraging them to adopt strong privacy and security practices that will protect personal data wherever it goes.

II. Background

Cross-border data flows foster innovation and growth, support cybersecurity, and enable access to essential services. They are important for delivering public services and empowering individuals to access them, including healthcare and education. Cross-border data flows make access to transformational technologies like AI equally available to individuals and public and private sector organizations who might otherwise be foreclosed from participating in this crucial aspect of the digital economy.[3] They foster collaboration and innovation using public data and data that is shared between organizations and between the public and private sectors, and they are crucial to the coordination of cybersecurity frameworks as well as the international effort to combat fraudulent and criminal activity in a number of sectors. In short, cross-border access to data is critical to enabling our modern digital ecosystem.

Data flows are also essential to economic growth. According to a 2021 Digital Economy Report by the United Nations Conference on Trade and Development, it has been estimated that global Internet traffic in 2022 alone will exceed all the Internet traffic up to 2016.[4] Such traffic is geographically concentrated in two main routes – between North America and Europe and North America and Asia. The World Trade Organization reported that trade in data-enabled services grew from $1.0 trillion in 2005 to $2.4 trillion in 2017.[5] According to the McKinsey Global Institute, "soaring flows of data and information now generate more economic value than the global goods trade" and have a larger impact on raising world GDP than the trade of goods.[6] Countries (and provinces) that participate in that flow show demonstrable economic benefits, while for those who "have been slow to participate, the opportunities for catch-up growth are too substantial to ignore."[7] Moreover, the International Data Corporation has predicted that 65% of GDP in 2022 will be digital,[8] and Leviathan Security Group found that organizations would pay 30 to 60% more for their computing needs if localization rules are adopted.[9]

Despite the economic and societal benefits of data flows, policy and law-makers and data protection authorities remain concerned with respect to data privacy and security protections for data in the exporting country. Many countries' data privacy laws contain restrictions on exports of personal data and provisions subjecting personal data flows to strict data transfer legal mechanisms. There is a consensus that privacy and security protections must flow with the data. Most recently, this concern has increased specifically with respect to disproportionate and excessive access to personal data by surveillance and intelligence agencies for national security purposes. In the EU, a 2020 case by the Court of Justice of the European Union,[10] followed by guidance from member state data protection agencies,[11] established a requirement for data exporters to conduct a local law assessment (or transfer risk assessment, "TRA") prior to transfers to countries that are not subject to an "adequacy" determination by the European Commission (EC).[12] The purpose of the TRA is to ensure that the import jurisdiction does not jeopardize the protection of the chosen (personal) data transfer mechanism, especially in respect of government use of data for national security, surveillance, and intelligence purposes.[13] The data exporter, in cooperation with the data importer, has the responsibility to perform these local law assessments and implement supplementary protective measures to mitigate the risks. According to the guidance of member state data protection agencies, if such supplemental measures do not eliminate such risks, the transfers should not

take place. Other jurisdictions, such as China[14] and the Dubai International Financial Centre (DIFC),[15] have implemented, or are considering implementing, similar transfer risk assessment requirements, although a great majority of the countries have not followed the EU Court doctrine in their national laws.

Based on the initial experiences of organizations conducting such local law or transfer risk assessments, the burdens they impose are substantial and unsustainable in the long run. This is a burden particularly for SMEs and public sector organizations, which lack the resources to conduct constant TRAs, but also for any large multinational company, given the increasing numbers of different data flows to many different countries and the fact that more jurisdictions may require some form of TRAs. If this approach is coupled with an expectation that transfers are only permitted upon a finding of no transfer risk after supplemental protective measures have been considered, (as the EDPB has suggested),[16] it may significantly diminish a broad range of essential and legitimate products and services both by private and public sector organizations. Key measures to counteract the problems of TRAs are a) to provide regulatory guidance and support for organizational TRAs and b) to enable a risk-based approach to data transfers with an assessment of the severity and likelihood of governmental use of data for national security, surveillance, and intelligence purposes in the importing country. Indeed, the UK Information Commissioner has signaled a more risk-based approach to data transfer risk assessments, and the UK government is proposing a more pragmatic approach to data flows as part of its UK data reform proposal of 2021.[17]

There is an undisputed large potential for societal benefits to be gained from international data flows. It is therefore imperative to engage in a thoughtful balancing of risks and benefits to avoid effectively localizing data or decreasing cross-border data flows and foreclosing many of the benefits.

This paper examines a "case study" of recent developments in British Columbia that appear to require a local law assessment (similar to a TRA) when using non-Canadian cloud services. In particular, this paper puts forward two policy-based propositions:

1. A local law assessment should be only one of many potential factors to be considered when transferring personal data outside of a jurisdiction; and

2. A local law assessment should not be required in instances where the security and privacy controls applied to the data (e.g., encryption in transit) sufficiently mitigate the potential risks of unauthorized access presented by local law, or the transferred data are historically and demonstrably of little interest to foreign governments.

Without these considerations embedded in any local law assessment rule, there is a significant risk of creating de facto data localization requirements and a reticence in engaging in activities that depend on global data flows. Data protection laws should aim to encourage good, privacy-protective behavior from companies *while* harnessing the benefits of data. It is possible to keep individuals' data appropriately safe and private while enabling beneficial data flows. This paper will propose an approach that could achieve both objectives.

III. Introduction to British Columbia Case Study

Until late 2021, public bodies in British Columbia and their service providers were required to comply with one of the most restrictive data residency laws in the world. The law required that "personal information in its custody or under its control is stored only in Canada and accessed only in Canada," unless limited exceptions applied.[18] The province of British Columbia passed this law in response to concerns about the

governmental use of data under the USA PATRIOT Act, and it explicitly applied to service providers and their employees as well.[19] It also required a public body or its service provider to notify "the minister responsible for this Act" if it receives "a foreign demand" for personal information, if it receives a request for disclosure that "it has reason to suspect" is for disclosure outside of Canada, or if it "has reason to suspect that unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure."[20]

In November 2021, these storage and access requirements were repealed and replaced with new provisions allowing a public body to disclose personal information outside of Canada if the disclosure is in accordance with any regulations promulgated under the same statute.[21] The British Columbia government made clear in a press release that the province's data residency rules were being updated "*so public bodies can use modern tools while continuing to protect personal information.*"[22] In effect, the province was acknowledging that the old rules were limiting the ability of public bodies, including universities, schools, and hospitals, to operate effectively in a digital world where data has to move across borders. The benefits of the amendments will include wider access to modern technology and tools, including cloud-based education and communication tools based outside of British Columbia. Associate Vice President, Information Technology, and Chief Information Security Officer of the University of British Columbia Jennifer Burns noted that the proposed amendments would "substantially increase the privacy and security of personal data with more robust and resilient services by allowing us to select the most secure and effective solutions."[23]

Subsequent regulations promulgated under the British Columbia statute and brought into force in late 2021 require the head of a public body to undertake a privacy impact assessment with respect to "each of the public body's programs, projects and systems in which personal information that is sensitive is disclosed to be stored outside of Canada."[24] Most recently, on March 4, 2022, the Office of the Information and Privacy Commissioner for British Columbia (OIPC) released guidance on security measures for personal information disclosures outside Canada. Significantly, the guidance includes a requirement that public bodies in British Columbia undertake an assessment of the legal framework in the jurisdiction where personal information is being disclosed or stored.[25] Furthermore, it includes a statement that "*[i]t is unlikely a public body would be able to meet its [safeguarding] obligations … when personal information under its control is processed or stored in a jurisdiction that does not respect the rule of law, has no privacy laws, or those laws are inadequate*."[26]

Although the guidance also includes a number of other risk-based factors (discussed below), it is uncertain whether or how these factors interplay with the local law assessment. This case study explores the potential impact of a local law assessment requirement and suggests principled policy reasons that support a narrow application of the OPIC's guidance on local law assessments and security measures for disclosures outside Canada.

IV. Local Law Assessments: What Are They and What Challenges Do They Create?

1. What is a local law assessment?

A local law assessment (also referred to as a transfer risk assessment or TRA) is an assessment of the laws of the jurisdiction into which the controller intends to transfer data to determine whether an adequate level of protection exists compared to the home jurisdiction. An increasing number of data protection laws limit data transfers to countries that offer similar, or essentially equivalent, protections for personal data. Within the EU, the European Commission ("EC") is competent under Art. 45 of the GDPR to designate

a third country, a more limited territory, or even just a sector in a third country, as essentially equivalent, allowing for mostly unhindered flows of personal data.[27] Art. 45 GDPR outlines the factors to be taken into account by the EC when conducting an adequacy assessment.[28] Organizations intending to transfer personal data into a country not afforded an adequacy decision by the EC and where no derogation under the law is available for their transfer, must carry out a TRA to identify any risks to the transferred data, including the risk of government access to the data for national security, surveillance, and intelligence purposes, and must consider mitigating measures. These TRAs are essentially small adequacy assessments of individual transfers, and the EDPB has issued extensive guidance on the steps involved in such an assessment."[29] Where the data exporter concludes that a risk is present, supplemental measures can be put in place to mitigate these risks.[30] If no effective mitigating measures to eliminate the risk can be identified as part of the TRA, a transfer may not take place or must be suspended under current EU law.[31]

Another example of these local law assessment requirements in addition to the one in British Columbia is Québec's Bill 64—An Act to Modernize Legislative Provisions as Regards to the Protection of Information. Under Section 27, the Act requires: "Before releasing personal information outside Québec, a public body must conduct a privacy impact assessment."[32] This assessment will take into account the sensitivity of the information, the purposes for which it will be used, the protection measures in place, and "the legal framework applicable in the State in which the information would be released."[33] Section 111 creates the same requirement applicable to a private sector enterprise before "communicating personal information outside Québec."[34]

It is important to note that while other countries contain restrictions on data transfers to countries without an adequate level of protection, a great majority do not explicitly require a local law assessment that includes consideration of national security, surveillance, and intelligence use of data.

2. What are the online services impacted by local law assessments?

An online service generally refers to any service provided over the Internet. Examples include services that provide email, text, or video conferencing where software and data are hosted or processed by the provider of the service. Online services also refer to services that provide computer infrastructure resources, including computing, storage, and networking, that are available on demand.

Online services have become pervasive in the marketplace. Whereas software solutions were previously licensed primarily for use within a customer's network infrastructure, most solutions are now delivered online. Online services are often provisioned using computing resources and infrastructure that are located in multiple jurisdictions. Many service providers locate computing infrastructure in multiple locations across national borders to achieve better performance (e.g., reduced latency), reach a broader range of customers, enhance cybersecurity, and mitigate climate, geopolitical, and other risks.

Restricting data flows can create challenges for effective, scalable, and protective delivery of online services. For example, in March 2019, the Institute of International Finance issued a report noting that such restrictions "may increase IT and data complexity; undermine the risk management, cyber security and anti-money laundering practices of financial institutions; as well as reducing access to financial services and markets in some countries."[35]

Examples of where the ability to use cross-border online services or the ability to process personal data across borders may be required (or strongly preferred) include:

- Enhancing cybersecurity protection,
- Enabling better fraud prevention and detection,
- Undertaking high volume computing with distributed networks, such as that required for natural language processing, cloud computing, or data analytics,
- Creating economies of scale for small businesses operating across borders, and
- Providing 24x7 customer support or remote support.

There are many other benefits of online services processing data outside of a country. Many "commonplace and essential tools and services that inherently, and by default, presume and depend on seamless global cross-border data flows" and the ability to access and process data globally.[36] These include tools for communication—for online education, online gaming, or hosting conferences—and tools for improving collaboration for activities such as humanitarian services or healthcare research.[37] Such benefits are not achievable in the absence of data flows in today's digital economy.

3. What challenges do local law assessments create in the context of online services?

It is a widely accepted general principle in data protection that protection must follow the data as it traverses national borders and that organizations must put in place accountability measures, including contractual and technical safeguards, for data processed by another entity and in another country. However, local law assessments create some noteworthy challenges in the context of online services. The results can lead to undesirable and unintended consequences for individuals and the public.

The majority of organizations using online services, both in the public and private sectors, are ill-equipped to undertake local law assessments. This is especially true for SMEs and start-ups, as these entities often do not have the required expertise, legal resources, and know-how to conduct such detailed analysis of the adequacy of foreign laws for every data flow they undertake. Yet, a McKinsey survey shows that 80 percent of start-ups are born global, as they use global technology, online services, and service providers, and even have global customers and consumers.[38] Furthermore, due to the global nature of computing infrastructure used to process data in connection with online services, organizations will often need to assess the laws of multiple jurisdictions. This is costly for any organization but can be particularly cost-prohibitive for small businesses. Indeed, organizations that have conducted such local law assessments under EU law consistently attest to the costliness and ultimate unsustainability of this requirement.

Such a requirement to conduct local law assessments, especially including the evaluation of the rules on government access and use of data for national security, surveillance, and intelligence purposes, could decrease the use of online services, thereby increasing cost to business, and could also potentially lead to the following various negative consequences:[39]

- *Lower Cybersecurity Protections*: Robust cybersecurity often relies on collecting and analyzing data for threat detection and trends throughout an entire ecosystem. For example, TrendMicro has a global database of emerging threats that is continuously updated to help identify suspicious activity or files and prevent cybersecurity incidents.[40] Cross-border data flows also enable a number of features for improved cybersecurity, such as partitioning sensitive datasets across global servers. Organizations that are not able to access cloud-delivered services would not be able to use such a tool, which could create more opportunities for hackers and reduce a layer of protection for business continuity and disaster recovery. If organizations cannot rely on cloud-based or distributed services, they may instead rely on centrally stored datasets that are limited to one jurisdiction and potentially overall less secure.

- *Hinderance to Business Continuity and Disaster Recovery*: Global data flows help enable threat detection, business continuity, and disaster recovery. When either a cybersecurity incident or a natural disaster occurs, online services can help organizations set up continuity services, recover datasets, and reduce overall downtime.

- *Increased Costs and Decreased Competitiveness*: The cost of creating redundant storage and not having access to modern cloud-based data storage solutions can create significant barriers for SMEs and start-ups and reduce access to the global market. The Business Council of Canada has expressed concern about restrictions on international data flows as having the potential to increase costs and reduce important efficiencies in processes, noting that Canadian companies often need to transfer "personal information of customers, employees and suppliers to multiple service providers around the world daily" in order to "take advantage of secure cloud computing and storage, as well as to support basic business processes, such as human resources, legal and shipping."[41]

- *Less Efficient Delivery of Digital Government Services*: Local law assessment requirements can create additional bureaucracy and less efficiency in delivering essential government services. After the 2004 data localization law passed, the Information Technology Association of Canada noted in the context of British Columbia that the reliance on geographic restrictions "led to more complex and time-consuming procurements, fewer service providers bidding on government business, and increased costs in delivering services to governments," and "the government is devoting more time and resources to procuring goods and services, while facing increased costs in delivering services to British Columbians."[42] The recent Covid crisis acutely demonstrated the need for governments to step up their efficiencies in the way they were monitoring and combating the spread of the virus and providing essential services to the public.

- *Decreased Innovation*: New technologies often require access to global data flows. For example, AI applications often rely on access and use of large, diverse, and global stores of data, especially for algorithmic training and to ensure algorithmic fairness, non-bias, and non-discrimination.[43] As the Ontario Chamber of Commerce noted, "This is a big challenge for AI firms in Canada, where a small population often makes it necessary to access foreign data to build robust AI models."[44] Unlocking the full potential of new technologies requires access to data for collaboration, research, and testing. Again, this need for data sharing was acutely felt during the global Covid pandemic, and data sharing was essential for managing the pandemic and enabling research and development for Covid vaccines. [45]

V. Why a Risk-based Approach to Local Law Assessments Is Critical

TRAs and other ex-ante transfer requirements are grounded in the important goal of protecting individual privacy and data protection, which have long traditions in many jurisdictions and are recognized as fundamental rights in some of them. It is therefore important to consider ways to offer robust and demonstrable protections for privacy and cybersecurity without removing the many benefits offered by processing and sharing data across jurisdictional lines. A risk-based approach to local law assessment requirements can achieve this goal and alleviate some of the substantial and unsustainable burdens otherwise associated with local law assessments.

A risk-based model for data protection acknowledges that privacy and data protection, while important fundamental human rights, must be safeguarded consistent with other rights and interests. This is the approach of other jurisdictions as well, and it has long been a hallmark of Canadian and British Columbian data protection law. The provincial Supreme Court of British Columbia emphasized that privacy is not an absolute right but is rather subject to a reasonableness test.[46] Canadian data protection laws require organizations to deploy safeguards to protect personal information against unauthorized access, use, or disclosure, but the nature of these safeguards will depend on the amount and sensitivity of the information, the method of storage, and other risk factors.[47]

Furthermore, by assessing the likelihood and severity of harms, risk-based local law assessments help governments and organizations identify mitigation strategies and ultimately reach an outcome that maximizes potential benefits while reducing the risk of harm.[48] A risk-based approach does not alter rights or obligations, but rather helps organizations comply with privacy requirements, prioritize actions, raise awareness about risks, and identify appropriate mitigation measures. The goal of such a risk management process—like all of effective data protection—is to provide for proportional responses that reduce the risk as fully as is practicable so as to assure legitimate benefits and identify mitigation strategies for any residual risks. A risk-based approach to local law assessments avoids preventing data transfers where the likely risks are low and/or are outweighed by the benefits.

VI. Implementing a Risk-based Approach in Practice

It is critical that policymakers and data protection authorities adopt a risk-based approach to any requirement for local law assessments rather than a strict rule that applies regardless of the specific circumstances. This is especially critical with respect to any requirements for an assessment to include an evaluation of the country's government access and use of data for national security, surveillance, and intelligence. It is well documented and evidenced by transparency reporting of many technology companies that such access to data is limited to specific services and sectors (communications, finance) and does not affect a great majority of everyday common types of personal data and transfers. Although local law assessments may theoretically have a role to play in managing privacy risks, they may not be necessary in all circumstances. A risk-based approach to local law assessments can achieve the dual goals of ensuring robust data protection while also enabling the benefits of cross-border data flows. To implement a risk-based approach to local law assessment requirements, there are two important considerations for policymakers:

1. A local law assessment should be only one of many potential factors considered when transferring information outside of a jurisdiction (see below); and

2. A local law assessment should not be required in instances where the security and privacy controls applied to the data sufficiently mitigate the potential risks of unauthorized access presented by local law, or where the transferred data are historically and demonstrably of little interest to foreign governments. (See below.)

Finally, it is important to clarify that a local law assessment is not designed to only enable cross-border transfer where there is no risk whatsoever; rather it is designed to identify material risks that must be addressed and mitigated as much as possible and in proportion to the expected economic and societal benefits. That clarification would substantially contribute to improving local law assessments.

VII. Applying a Risk-based Approach in British Columbia

1. Consideration of additional risk factors (other than local law of a third country)

Local law should only be one of many factors for exporting organizations to consider when transferring information outside of a jurisdiction. The Office of the Information and Privacy Commissioner of British Columbia's guidance on reasonable security measures for personal information disclosures outside Canada ("OIPC Guidance") already acknowledges that additional factors can play a role. The guidance specifically notes, "Other factors that should be assessed, depending on the circumstances, include:

- the sensitivity of the personal information in question (e.g., personal health information is much more sensitive than contact information);
- the volume of the personal information in question;
- the foreseeability of an unauthorized collection, use, disclosure, or storage of personal information;
- the impact to individuals of an unauthorized collection, use, disclosure, or storage of their personal information;
- whether the personal information is stored by a service provider; and
- whether a reasonable alternative is available within Canada."[49]

In CIPL's response paper to the EU Court decision on essential equivalence requirements for data flows to third countries, we also noted a number of similar and additional factors that organizations already take into account as a matter of accountability.[50]

Finally, it is also important to consider the benefits of transferring data across borders and the impact of not realizing such benefits, and whether there are other means of protecting data and mitigating any risks from local laws. Moreover, some of the other risk factors in the above list, such as the "foreseeability of an unauthorized collection, use, disclosure, or storage of personal information" may obviate the need for a local law assessment altogether. Thus, for example, where an organization can demonstrate for certain types of data a very low historical risk of inappropriate government access in a foreign jurisdiction or other inappropriate access, disclosure, or use, the organization should not have to undertake a formal local law assessment at all.

2. Consideration of additional safeguards and controls

These factors—particularly the sensitivity of the information, the foreseeability of an unauthorized collection, use, disclosure, or storage of personal information, and the potential harm caused by unauthorized disclosure—are considerably important not only when assessing local laws, but generally when the organization is considering the parameters for safeguards to protect the relevant data. The OIPC Guidance also acknowledges the privacy-protective benefits of administrative, technical, or contractual controls, noting that public bodies should deploy such controls and "be prepared to demonstrate reasonable security controls in line with industry standards such as ISO 27002, ISO 27017, or the NIST Cybersecurity Framework."[51] However, the Guidance recommends local law assessments regardless of technical or other safeguards in place.

In some cases, a risk-based analysis may demonstrate that the risks are sufficiently mitigated by technical, organizational, and contractual controls that an organization has in place. When data is already substantially protected by such measures, a local law assessment should not be required. These controls

may include, for example, using encryption in transit, obtaining certifications to international standards such as ISO/IED 27001/27018, using pseudonymization for sensitive data, and other technical and contractual measures.[52]

3. PIPEDA's and the OECD's accountability-based approach to data flows

One model for data flows that may be helpful is the OECD's outline of basic principles for the free flow of data and legitimate restrictions. The first of these is that a "*data controller remains accountable for personal data under its control without regard to the location of the data*."[53] Indeed, this is Canada's approach to data transfers under its Personal Information Protection and Electronic Documents Act (PIPEDA).[54] Under the 2009 Guidelines for Processing Personal Data Across Borders,[55] organizations that transfer personal data from Canada to a service provider in another jurisdiction must ensure through contractual or other means that the data continues to be protected at a level that is comparable to the level at which it would be protected should it remain within the organization. Under this model, individual organizations are held accountable for what happens to the personal data they transfer and must ensure that their service providers deliver adequate protection regardless of where they are located. The other relevant OECD principles highlight the importance of considering sufficient safeguards, including enforcement mechanisms and measures put in place by the data controller, as well as accounting for the sensitivity of the data and the purpose and context of the processing. [56]

Following a similar risk-based accountability approach would enable the benefits and efficiencies of online services while also being highly protective of data. The issue is not a choice between the benefits of online and cloud-based services or robust privacy protections—it is how to enable the flourishing of both.

VIII. What Lessons Can We Take from This Case Study?

This case study demonstrates how deploying a risk-based model can foster good data protection practices by encouraging enhanced privacy and security standards without being too prescriptive or prohibitive. Policies and regulations can allow for greater free flows of data in the context of historically low-risk transfers, or when organizations have made privacy-protective decisions and have certain technical, physical, or administrative measures in place. This allows organizations to utilize resources more effectively to protect privacy and security while also allowing individuals and organizations to benefit from the numerous significant advantages offered by cross-border data flows. Widespread adoption of this risk-based approach would also help achieve the global interoperability of data flows, further unlocking the sustained economic and societal benefits offered by modern technologies and online services.

---

[1] Bill 22—Freedom of Information and Protection of Privacy Amendment Act, 2021, https://www.leg.bc.ca/parliamentary-business/legislation-debates-proceedings/42nd-parliament/2nd-session/bills/progress-of-bills.

[2] Office of the Information and Privacy Commissioner of British Columbia, *Reasonable Security Measures for Personal Information Disclosures Outside Canada* (March 2022), https://www.oipc.bc.ca/guidance-documents/3646.

[3] For example, small and medium enterprises (SMEs) and start-ups are able to gain access to global markets and supply chains, enabling data-driven innovation and expanding competition. Cross-border data flows are also important to enhance access to finance, promote agricultural sustainability and productivity, and improve access to health care. Global Data Alliance, *Cross-Border Data Transfers & Economic Development: Access to Global*

Markets, Innovation, Finance, Food, and Healthcare, International Development Series No. 1 (2021), https://globaldataalliance.org/wp-content/uploads/2021/07/05062021econdevelopments1.pdf.

[4] United Nations Conference on Trade and Development (UNCTAD), *Cross-border data flows and development: For whom the data flow*, Digital Economy Report 2021 (2021), https://unctad.org/system/files/official-document/der2021_en.pdf.

[5] World Trade Organization, *World Trade Report 2019: The Future of Services Trade*, Figure D.6: Global exports of ICT-enabled services (2019), https://www.wto.org/english/res_e/booksp_e/00_wtr19_e.pdf, p. 89.

[6] McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows* (2016), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

[7] Id.

[8] International Data Corporation, *IDC FutureScape: Worldwide Digital Transformation 2021 Predictions* (2020), https://www.idc.com/getdoc.jsp?containerId=prUS46967420.

[9]Leviathan Security Group, *Quantifying the Cost of Forced Localization* (2015), https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

[10] Judgement of July 16, 2020 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* C-311/18 (*Schrems II*).

[11] European Data Protection Board (EDPB), *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (2021), https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[12] Adequacy findings establish that the data protection framework of the third country provides protections that are "substantially equivalent" to the protections under relevant EU law. *See* Adequacy Decision, Art. 45 GDPR.

[13] The General Data Protection Regulation (GDPR), Europe's data protection standard, requires that, where a third country has not been recognized by the European Commission as having a level of adequate data protection, the standard of data protection has to be maintained as data travels across borders by using certain data transfer tools available in Art. 46 GDPR.

[14] Article 38, China Personal Information Protection Law (PIPL), http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

[15] DIFC, *Consultation Paper: Non-Legislative Proposal on Updated Data Export Tools & Guidance* (April 2022), https://dg23rp0isu1uj.cloudfront.net/application/files/2416/4986/9067/Non-leg_Consultation_-_April_2022_Export_EDRMI.pdf.

[16] Supra note 11.

[17] UK Department for Digital, Culture, Media & Sport (DCMS), *Data: a new direction, Chapter 3 - Boosting trade and reducing barriers to data flows* (2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf.

[18] Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004, https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00_multi.

[19] Id. § 30.4.

[20] Id. § 30.2(2).

[21] Bill 22—Freedom of Information and Protection of Privacy Amendment Act, supra note 1.

[22] *News Release: Amendments strengthen access to information, protect people's privacy*, Ministry of Citizens' Services, British Columbia (October 2021), https://news.gov.bc.ca/releases/2021CITZ0048-001990/.

[23] Id.

[24] Personal Information Disclosure for Storage Outside of Canada Regulation, BC Reg 294/2021, Freedom of Information and Protection of Privacy Act (2021), https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/294_2021.

[25] OIPC Guidance, supra note 2.

[26] Id.

[27] There are currently 14 of such adequacy decisions in existence, including for commercial sectors in Canada. European Commission, *Adequacy Decisions*, https://ec.europa.eu/info/law/law-topic/data-

protection/international-dimension-data-protection/adequacy-decisions_en. The EU-US Privacy Shield, a separate mechanism for exporting data to certain sectors in the US, was annulled by the *Schrems II* decision.

[28] These include, for example, reviewing the rule of law, respect for human rights and fundamental rights, judicial redress for individuals, and the presence of an independent supervisory authority, to name a few.

[29] European Data Protection Board, *Recommendations 01/2020 on measure that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0)* at para. 30 (18 June 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[30] Id., p. 20.

[31] Id., p. 26.

[32] Bill 64—An Act to Modernize Legislative Provisions as Regards to the Protection of Information, National Assembly of Québec (2021), http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2021C25A.PDF.

[33] Id.

[34] Id.

[35] Institute of International Finance, *Data Flows Across Borders: Overcoming Data Localization Laws* (2019), https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf.

[36] CIPL, *Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (21 December 2020), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_edpb_supplementary_measures_recommendations__21_dec_2020_.pdf, at p. 6.

[37] Id., p. 6-7. For example, according to the Global Data Alliance, "cross-border data analytics can help speed the early identification of potentially useful drug candidates, shortening pharmaceutical discovery timelines from years to months" and saving up to $26 billion in costs. Global Data Alliance, *Cross-Border Data Transfers & Biopharmaceutical Research and Development* (2021), https://globaldataalliance.org/wp-content/uploads/2021/09/09092021cbdtbiopharma.pdf.

[38] Supra note 6.

[39] CIPL has previously outlined some of these negative consequences in: *Enabling Accountable Data Transfers from India to the United States Under India's Proposed Personal Data Protection Bill (No. 373 of 2019)*, Centre for Information Policy Leadership and Data Security Council of India (August 2020), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-dsci_report_on_enabling_accountable_data_transfers_from_india_to_the_united_states_under_indias_proposed_pdpb__8_september_2020_.pdf, p. 7-8.

[40] TrendMicro, *Global Threat Research*, https://www.trendmicro.com/en_us/about/threat-research.html.

[41] Business Council of Canada, *Data Driven: Report and Recommendations* (2020), https://thebusinesscouncil.ca/report/data-driven/.

[42] Information Technology Association of Canada, *The USA Patriot Act and the Privacy of Canadians* 5 (July 2005).

[43] *See* CIPL, *First Report: Artificial Intelligence and Data Protection in Tension* (October 2018), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf.

[44] Ontario Chamber of Commerce, *In Data We Trust: Unlocking the Value of Data in Ontario* (2020), https://occ.ca/wp-content/uploads/OCC-DataReport.pdf.

[45] *See* CIPL, *Covid-19 Meets Privacy: A Case Study for Accountability* (14 April 2020), https://www.informationpolicycentre.com/cipl-blog/covid-19-meets-privacy-a-case-study-for-accountability.

[46] "The importance of the right to privacy . . . cannot be minimized. Those fundamental rights are contained in the Charter for the benefit of all Canadians. However, those rights, as previously stated, are not absolute. There is a reasonable expectation of privacy and the language [of the Charter] emphasizes that individuals should be secure against unreasonable search and seizure. In the case at bar . . . . [t]he reasonable expectations of privacy are satisfied by statute and by contract. . . . A reasonable expectation of privacy is protected." BC Government & Service Employees' Union v. British Columbia (Minister of Health Services), 2005 B.C.S.C. 446 ¶¶ 68-70.

[47] As another example, the breach notification requirement in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) requires notification when a breach of security safeguards "creates a real risk of significant harm" to an individual. Office of the Privacy Commissioner of Canada, *What you need to know about mandatory reporting of breaches of security safeguards* (2021), https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.

[48] International Organization for Standardization, *ISO 31000:2009 Risk management—Principles and guidelines*. *See also* supra note 36, p. 9-14.

[49] OIPC Guidance, supra note 2.

[50] These factors include:

- Nature of the data being transferred;
- Nature of the data processing subject to transfer;
- Categories of data subjects and the impact of the processing and transfer on them, including severity and likelihood of harm if data is accessed by unauthorized third parties;
- Likelihood of government access to certain types of data and whether the data that is subject to the transfer is within the scope of intelligence and law enforcement activities;
- Volume of data transferred, including number of data subjects covered;
- Purpose of the data transfer;
- Volume of data potentially impacted relative to the overall volume of data transferred;
- Organizations' business model, and the business sector in which the transfer takes place;
- Nature of the transfer;
- Duration and frequency of the transfer;
- Technical controls and organizational measures in place or possible safeguards;
- Type of data recipient;
- Number, type and location of processors and sub-processors involved in the transfer;
- Existence of a DPO or Chief Privacy Officer within the data importer's organization; and
- Data importer's membership or public support to organizations advocating for the defense of human rights.

See CIPL, *A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision* (2020), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf. See p. 8-10 for additional information on these risk factors.

[51] OIPC Guidance, supra note 2.

[52] CIPL's research and survey has explored a wide array of tools available to organizations to consider, including legal measures (contractual measures), organizational measures (risk assessments, data minimizations, certifications and codes of conduct, transparency reports, etc.), and technical controls (comprehensive security infrastructure, access controls, anonymization/pseudonymization, access controls, etc.). Supra note 50, p. 11-15.

[53] OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[54] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, https://canlii.ca/t/541b8.

[55] Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders* (2009), https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/.

[56] The other two principles are: "A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines;" and "Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing." Id.