Home Ice Advantage

Securing Data Sovereignty for Canadians on Social Media

November 2020

Yuan Stevens | M.J. Masoodi | Sam Andrey

cybersecure policy exchange

Powered by RBC

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is a new initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation.

Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Ryerson University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.

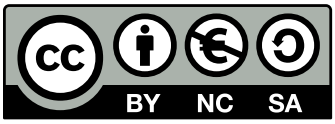
Ryerson Leadership Lab

The Ryerson Leadership Lab is an action-oriented think tank at Ryerson University dedicated to developing new leaders and solutions to today's most pressing civic challenges. Through public policy activation and leadership development, the Leadership Lab's mission is to build a new generation of skilled and adaptive leaders committed to a more trustworthy, inclusive society.

This initiative is made possible by the generous contributions of Royal Bank of Canada, which enable our team to independently investigate pressing public policy issues related to cybersecurity and digital privacy. We are committed to publishing objective findings and ensuring transparency by declaring the sponsors of our work.

How to Cite this Report
Stevens, Y., Masoodi, M.J. & Andrey, S. (2020, November). *Home Ice Advantage: Securing Data Sovereignty for Canadians on Social Media*. Cybersecure Policy Exchange. Retrieved from: https://www.cybersecurepolicy.ca/datasovereignty

350 Victoria St, Toronto, ON M5B 2K3
ISBN: 978-1-77417-022-9



Contributors
Sam Andrey, Director of Policy & Research, Ryerson Leadership Lab
Karim Bardeesy, Executive Director, Ryerson Leadership Lab
Sumit Bhatia, Director of Communications and Knowledge Mobilization, Rogers Cybersecure Catalyst
Zaynab Choudhry, Design Lead
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Braelyn Guppy, Marketing and Communications Lead, Ryerson Leadership Lab
Mohammed (Joe) Masoodi, Policy Analyst, Ryerson Leadership Lab
Yuan Stevens, Policy Lead, Ryerson Leadership Lab

Our work is guided by these core principles:

- Responsible technology governance is a key to Canadians' cybersecurity and digital privacy.
- Complex technology challenges call for original insights and innovative policy solutions.
- Canadians' opinions matter, and must inform every discussion of technology policy.
- Cybersecurity needs to be explained and made relevant to Canadians, and cannot be relegated to language and concepts accessible only to experts.
- Canadian institutions matter, and must evolve to meet new cybersecurity and digital privacy risks to maintain the public trust.
- Harms, inequities and injustices arising from the unequal use or application of technology must be confronted, wherever they exist or could arise.

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange
For more information, visit: https://www.cybersecurepolicy.ca/

Executive Summary

More than three in four Canadians use social media platforms to connect with others here at home and around the world, often sharing life's most intimate moments through public posts and private messages. In doing so, Canadians entrust these companies to secure and protect their personal data, which can include a wide range of sensitive information, such as their political opinions, or details on their sex life, personal finances and health. These companies are also entrusted to secure the sensitive data that they track and store, such as users' location, search histories and biometric information such as facial features.

But that trust is waning. Our surveys of Canadians indicate that **social media platforms are the least trusted organizations in Canada** to keep personal data secure and to act in the best interests of the public. As legal battles swirl between Europe, the U.S. and China over how to protect Facebook and TikTok data travelling across borders, there remain inadequate protections over how Canadians' personal data are transferred and stored.

This threatens Canadian sovereignty, and the digital security and privacy of millions of Canadians. Personal data can be accessed by national security and law enforcement agencies without sufficient legal protection under Canadian law in countries around the world. Technology companies can experience buy-outs, mergers and bankruptcy that can change where personal data are stored and the privacy protection they receive. Malicious hackers can also take advantage of data stored in locations where the data are subject to weak data protection safeguards.

Social media platforms store the personal data of their Canadian users around the world, and provide **little to no transparency** as to where their data are stored or transferred to third parties. Canadian privacy law does not require users to consent to personal data transfer outside of Canada. Our research shows that **many popular platforms transfer data to a variety of jurisdictions, and none specifically cite Canada as a country of storage.**

Nor are there meaningfully enforced limits on the transfer of personal data to jurisdictions with **insufficient protection** against surveillance or unauthorized access. **In the two decades since the enactment of Canada's current privacy law, there has not been a single fine or enforced remedy against companies transferring personal data outside of Canada with insufficient protection.**

Jurisdictions around the world are introducing a range of new approaches to address these challenges and ensure data protection laws extend to data moved outside its borders, including outright bans on cross-border transfer, new requirements for informed consent, and rigorous evaluations of other jurisdictions' data protection regimes. While these notions can challenge the idea of a free and open Internet, Canadians are looking for answers — our recent survey finds that **86% of Canadians support** requirements to keep Canadians' data within Canada.

86%

of Canadians support requirements to keep Canadians' data within Canada.

This discussion paper lays out public policy options for how **Canadian privacy law should protect the security and privacy of personal data stored outside of Canada:**

1. **Comparable Protection:** Provide precise requirements and enforcement to ensure social media personal data receive comparable levels of protection when transferred outside of Canada;
2. **Consent:** Require social media platforms to obtain explicit consent from Canadians for the transfer of their personal data to jurisdictions that do not provide comparable protection, providing information about the specific data and countries involved; and
3. **Sensitive Data:** Better define and provide greater security protections for sensitive personal data, such as private messages and biometric data.

Policy-makers wrestling with how to evolve Canadian privacy law in the social media age face an immense challenge, and opportunity, to make foundational policy changes that can protect Canadians' privacy and security. It is critical that we modernize our laws to ensure the principle of adequate protection from unauthorized access to our personal data. And it is urgent to uphold privacy rights as we move vast amounts of personal data to countries around the world.

Canadians should have assurance that the jurisdictions where their data are transferred protect and enforce their rights, and enforce those protections. They should have transparent information to inform their decisions. And they should have confidence that their most sensitive data will never be compromised.

Advancing these protections for Canadians should complement ongoing efforts to advance international cooperation and governance of digital privacy and security, for example through bi- and multilateral agreements. The global fight over data is likely only to intensify in the coming years, and a key test for Canada's sovereignty will be how it is positioned among its international peers. Canada must define its position internationally, with the U.S., China, and the European Union all showing very different models of governance.

This paper is meant to advance public engagement and policy development in Canada going forward to maintain our "home ice advantage."

Intent of This Report

This discussion paper analyzes considerations and provides policy options on the issue of data sovereignty, focusing specifically on Canadians' personal data that are collected and stored by social media platforms. The paper is informed by a literature review, interviews and a representative survey of Canadians. This paper, and the ones to follow, are intended to inform and generate feedback from stakeholders, experts and the public on the options available to Canadian policy-makers on pressing matters as Canada's jurisdictions review how to update our privacy laws governing social media platforms.

Introduction

Nine years ago, Max Schrems was studying law in Austria and did a semester abroad at Santa Clara University in Silicon Valley. It was there that Schrems heard Facebook's lawyer Ed Palmieri speak to one of his classes, and where he was struck by Palmieri's understanding of European privacy law. He decided to write his thesis paper on Facebook's privacy practices. In the course of his research, he accessed 1,200 pages of his personal data collected and stored by Facebook, which had been transferred from its European headquarters in Ireland to the U.S. By the time he was back in Austria in 2013, the Edward Snowden leaks had accused the U.S. National Security Agency (NSA) of bulk-collecting personal data from communication service providers, including Facebook. Angered at the prospect that his detailed personal data, and the data of millions of people in Europe who had ever used Facebook's services, had been under surveillance, Schrems filed a complaint against Facebook with the Irish Data Protection Commissioner, aimed at stopping European data transfer to the U.S.[1]

This began a journey of legal battles spanning several years, ending with the European Union's highest court. In July 2020, the European Court of Justice analyzed the legal framework of the NSA's mass surveillance programs, and held that the U.S. had failed to limit the scope and application of the NSA's surveillance, or to provide actionable data protection rights related to the NSA's surveillance.[2] The court's landmark decisions struck down two significant legal mechanisms that allowed companies to 'self-certify' their adherence to data protection principles. In doing so, the court eliminated the presumptions that personal data transferred from the EU to the U.S. receive adequate levels of protection or are subject to appropriate safeguards required under EU privacy law.[3] The legal battle continues. Despite a preliminary order in September 2020 prohibiting the company from transferring its EU user data to the U.S., Facebook has successfully argued against the order and continues its data transfer, while Schrems continues his legal battle.[4]

At the same time, the U.S. has taken its own dramatic action to prohibit the transfer of personal data outside its borders. President Trump signed executive orders in August 2020 to block Chinese social media apps TikTok and WeChat in the U.S. The executive order cited that TikTok's "data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information."[5] A U.S. judge put the WeChat ban on hold, citing potential violations of freedom of speech rights; while the TikTok ban was also put on hold pending a potential restructuring that would have American user data stored in the U.S.[6]

India made a similar move in June 2020, blocking TikTok and WeChat, citing national security concerns from "stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India."[7] The EU has since launched an investigation into TikTok.[8] At the same time, Misty Hong, a student in California, has filed a new lawsuit alleging TikTok sends users' personal data to China that are subject to government surveillance. She claims that she never created an account after downloading the app, and that her personal data, including her biometrics from videos created but not posted, were later transferred to servers in China.[9]

At the heart of these legal tugs-of-war are several cross-cutting issues that policy-makers around the globe — including in Canada — are faced with today. Who bears responsibility for ensuring the privacy and security of our data? More specifically, can organizations be trusted to self-regulate, or should they be subject to regulation, oversight and enforcement when it comes to safeguarding the privacy and security of personal data?

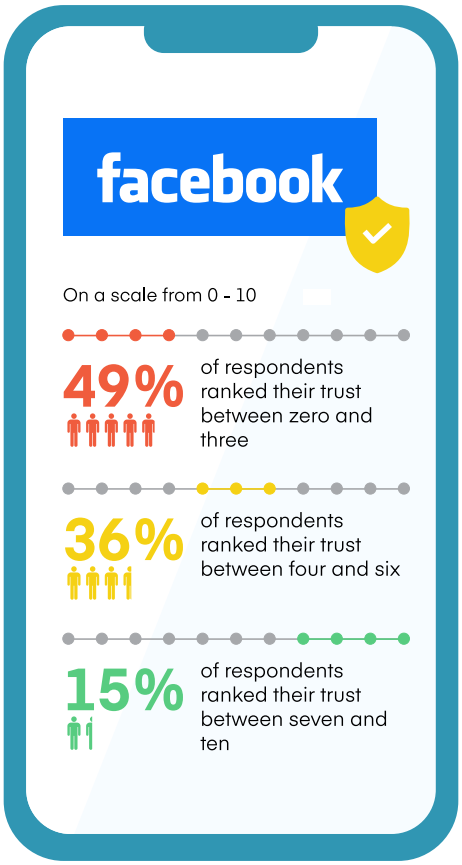
Further, when organizations rely on remote storage for enormous amounts of personal data, which privacy, data protection and surveillance laws apply? In other words, do a person's data protection rights travel with their personal data, or does the transfer location of personal data determine the privacy protection, if any, that this data will receive? Should certain kinds of data — for example, biometric data, political opinions, details about people's sexual orientation or sex life, or data that reveal information about their health or that of their families — be treated with special care because of their sensitive and revealing nature?

These questions of data sovereignty often centre on protecting confidential or personal data held by governments, such as sensitive health and financial information, or information related to national security. While treatment of data entrusted to government is important, it is also much more regulated in Canada at the federal and provincial levels.

However, in many respects the personal data of Canadians collected, stored and used by social media platforms are as sensitive and vulnerable to misuse as are most personal data stored by governments — and are mostly governed by one piece of legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which has not been substantially updated in two decades.

The seemingly mundane topic of data storage is therefore a critical issue for Canadian policy-makers. Canadians who responded to two of our surveys in the past year tend to agree. When we asked Canadians in August 2019 the degree to which they trusted 27 different organizations to act in the best interests of the public, Facebook, Twitter and Instagram had the lowest levels of trust — earning less trust than oil companies and telecommunication providers.[10] Similarly, when we asked Canadians in May 2020 to rank on a scale of zero to ten the level of trust they placed in different organizations to keep their personal data secure, Facebook had the lowest levels of trust, with 49% of respondents ranking their trust in the company between zero and three and only 15% of people ranking Facebook above six.[11]

Canadians' Trust in Facebook to Keep Data Secure



How companies store our personal data is a chief security concern, especially when it comes to social media platforms. In August 2019, 84% of Canadians reported that the security of their personal data from cyberattack was a problem affecting Canadian society — a greater proportion than that who worried about the state of the economy.[12] There is good reason for Canadians' lack of confidence. Over the last five years, major security breaches have impacted nearly every major social media platform, including Facebook, Instagram, LinkedIn, Snapchat, Twitter and TikTok.[13] Six security breaches of social media platforms accounted for 56% of the total 4.5 billion records compromised worldwide in 2018 — such as the infamous Cambridge Analytica-Facebook data leak that compromised the personal data of 87 million Facebook users, including more than 600,000 Canadians.[14]

Social media platforms face a wide array of security threats that are impacted by the storage and transfer location of personal data. Facebook's partnership with Cambridge Analytica, which Zuckerberg admitted was a "breach of trust," demonstrates the enormous risks of trusting social media companies to self-regulate — particularly when they allow third parties to develop platform applications or provide core infrastructural needs such as data storage.[15]

In other words, even the most well-resourced private corporations on the planet are, on occasion and to great consequence, unable to deliver on the privacy protections they promise.

In the case of Schrems, the security of Facebook users' personal data was called into question by government agencies' access to this data for purposes such as national security or law enforcement. Recent changes to national security and surveillance law in Hong Kong also underline how rapidly the security of data stored abroad can change.[16] Malicious hackers can also take advantage of data stored in locations where the data are subject to weak data protection safeguards. Technology companies also regularly experience buy-outs, mergers and bankruptcy, which can alter where personal data are stored and the privacy protection it receives outside the reach of Canadian regulators.[17]

Jurisdictions around the world are introducing a range of new approaches to address these challenges and protect personal data transferred outside its border, including outright bans on cross-border transfer, new requirements for informed consent and evaluations of other jurisdictions' data protection adequacy. These sorts of legal limits can challenge the notion of a free and open Internet.[18] However, existing protections in Canada have proven inadequate to rapidly changing circumstances outside our borders.

This report first reviews how social media platforms collect consent and store Canadians' data. It then provides an overview of the current laws in Canada and abroad concerning the storage and transfer location of personal data. We then analyze the legal, business and privacy implications of policy options for data sovereignty as private sector law is overhauled in Canada. Finally, we recommend that Canadian policy-makers implement new protections in order to adequately protect the privacy and security of Canadians using social media platforms.

Key Terms and Scope

Throughout this paper, we refer to the following key terms and concepts, which we define in the following ways:

Social media company or platform: There is no single definition of social media; however, for the purposes of this paper, we define social media as an online service that allows individuals to (1) create a public or semi-public personal profile; (2) maintain and view a list of other users with whom they are connected to; and (3) share or publish (rather than merely consume) content.[19]

This paper focuses on the data storage and transfer practices for the following social media platforms, which Canadians reported using most often this year: Facebook (including its subsidiaries Instagram and WhatsApp), LinkedIn, Pinterest, Snapchat, TikTok and Twitter.

Social media data: According to their privacy policies, social media platforms collect, process and/or transfer a wide range of data, including:

- Personally identifying information (e.g., name, phone number, address, date of birth);
- Public and private posts and messages, which can include a wide range of sensitive information and images, videos and audio;
- Location information;

Social media companies may conceivably be for-profit or not-for-profit, which is currently an important distinction in Canadian privacy law: for example, federal privacy law generally does not apply to not-for-profit or charitable organizations, whereas private sector privacy laws in Alberta and British Columbia generally apply to not-for-profit organizations. For the purpose of this report, we assume that social media platforms are subject to private sector privacy law in Canada.

Which Social Media Platforms Are Canadians Using?

- Facebook 69%
- Facebook Messenger 55%
- Instagram 42%
- WhatsApp 33%
- LinkedIn 27%
- Twitter 25%
- Pinterest 21%
- Instagram Direct Messages 17%
- Snapchat 17%
- Reddit 12%
- TikTok 10%
- Twitter Direct Messages 5%
- WeChat 4%
- Telegram 2%
- Signal 1%

from March to May 2020

- Financial information (e.g., credit card transactions);
- Biometric data, such as facial feature vectors created by face recognition technology to identify individuals in photos or videos;
- Log data (e.g., IP address, cookie ID, referring web pages, pages visited, mobile carrier and device information, search history); and
- Personal data obtained from other sources, such as advertisers, web browsers, calendars, other social media platforms and other third parties.

Social media personal data: Data collected by social media platforms that could, by itself or when combined with other data, be used to identify an individual.

Canada's federal and provincial privacy laws generally use the term "personal information" and apply a relatively broad interpretation to mean information about an individual, including where there is a serious possibility that an individual could be identified through the use of that information alone or in combination with other information.[20]

In the European Economic Area, the General Data Protection Regulation (GDPR) provides protection for "personal data," which is defined as data 'related to' an individual.[21] We use this term in the paper, as we believe it more accurately shapes the object of protection by policy-makers, the justice system and the public.[22]

Data localization: Sometimes also referred to as data residency; a term meaning legal requirements that data reside and be stored in the country or jurisdiction in which they are collected.

Data sovereignty: The notion that data should be subject to the laws and governance of the nation within which the data are collected — which is challenged when data are transferred, stored and/or processed outside of the country of collection.[23] For some, the term data sovereignty is used interchangeably with the notion of data localization,[24] but in the context of this paper it is treated as a separate policy challenge that can involve a number of solutions.

Data subject: An individual person who can be identified, directly or indirectly, by their social media personal data.[25] In this paper, when we refer to "Canadians," we mean to include all data subjects generating from data collection or use while in Canada, regardless of citizenship or residence.

The term "data sovereignty" is also used in Canada in an Indigenous context, generally referring to efforts by First Nations individuals and communities to have sovereignty over data collected about First Nations peoples by governments and/or researchers, according to the principles of Ownership, Control, Access and Possession (OCAP). While a very important topic, this is also beyond the scope of this paper.

Data processing: A robust definition of this term means any operation performed on personal data, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination or otherwise making available, combination, restriction, erasure or destruction.[26] The dichotomy of "use" and "disclosure" has led to significant debate in Canadian privacy law because private sector organizations in Canada must currently obtain consent from the data subject for when they "disclose" personal data, but are not required to obtain consent if the data are transferred to a third-party service provider.[27]

Out of scope for this paper: A final note that this paper is focused on the question of transfer and storage outside of Canada; and questions related to individual data ownership, portability or erasure, and their relationship to third-party transfer and use are important but beyond its scope. A particular public policy challenge is the ability for public and private entities, emboldened by machine learning systems, to scrape social media platforms of publicly posted data. They can then aggregate and generate new data sets, that can be housed outside Canada, that could, in their existence and use, threaten the security and privacy of Canadians regardless of data storage laws.

Also out of scope is the treatment and sovereignty of the myriad other forms of data that Canadians generate while online, but that is not social media data (e.g., email traffic and financial transactions run through platforms that are not integrated with social media platforms; audio or visual information collected through phones and other connected devices that are not posted to social media platforms).

Social Media Data Storage Practices

Increasing volumes of data are stored on servers around the globe. To address the costs and operational challenges of ever-increasing data collection, it is now common for private and public institutions to outsource their data storage through on-demand cloud-based services, where data servers are not necessarily located in the country of the data subject or presiding jurisdiction.[28] There are numerous service and deployment models for cloud-computing, and examples of major cloud data storage companies include Amazon Web Services, Google Cloud and Microsoft Azure.[29] In general, the location of data centres can take into consideration a variety of factors, including proximity to users and skilled labour, electricity costs, risk of natural disasters, redundancies, security and local laws.

Our research demonstrates that most social media platforms' privacy policies **do not disclose** precisely which jurisdiction they store, process and transfer the personal data of a given user. Instead, social media privacy policies generally provide for the ability to store personal data in any country chosen by the social media company, unless a country or region's law requires otherwise. This also means that social media platforms can easily transfer personal data between various countries with little oversight or transparency. As we can see from the following infographic, social media platforms are often not transparent about where they store and transfer the personal data of Canadian users; and **none specifically cite Canada as a country of storage** or transfer for the personal data of Canadian users.

In many jurisdictions, personal data stored in other countries can be obtained through a warrant, court order or subpoena request from a foreign law enforcement agency; and under some foreign laws, disclosure could take place without notice to the user.[30] For example, the U.S. *Foreign Intelligence Surveillance Act* can compel a communications service provider, subject to U.S. law, to turn over data under its control. In China, the Cybersecurity Law, implemented in 2017, advances the principle of cyber-sovereignty which assumes that the Internet is subject to state sovereignty.[31] The U.S.'s FBI has warned that the law could force companies that store or transmit data through servers in China to surveillance measures.[32]

The privacy policies from three of the social media platforms we reviewed make this ease of access explicit. LinkedIn's Privacy Policy tells users that countries to which their data have been transferred "may have laws which are different from, and potentially not as protective as, the laws of your own country."[33] Pinterest tells users that "privacy protections and the rights of authorities to access your personal information in such countries may not be equivalent to those of your home country."[34] Likewise, Twitter tells its users that "the privacy and data protection laws and rules regarding when government authorities may access data may vary from those of your country."[35]

All of the social media platforms reviewed state that they do not sell users' personal data; however, each indicates that it provides personal data access to third-party partners, affiliates and/or service providers. Each also warns users that personal data could be shared in the event of a sale, merger or acquisition.

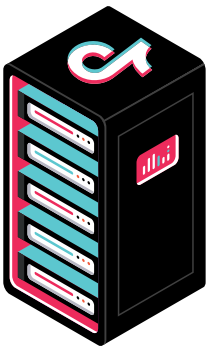
Policy-makers should not find it surprising that social media platforms store and transfer the personal data of Canadian users without oversight. The next section identifies gaps in Canada's private sector personal data laws.

Company policy on the personal data storage of Canadian users

Facebook

Facebook's Data Policy states that user information and data may be stored or transferred "in the **United States or other countries**" outside of where users live.[36]

In 2019, Mark Zuckerberg wrote that "[p]eople should expect that we won't store sensitive data in countries with weak records on human rights like privacy and freedom of expression in order to protect data from being improperly accessed." [37] However, no publicly-available policy clarifies this.



TikTok

TikTok's Privacy Policy states that they store and transfer user data "in **Singapore** or **in the United States**, outside of the country where [users] live."[38]

Prior to 2019, TikTok's Privacy Policy stated: "We will also share your information with any member or affiliate of our group, **in China**, for the purposes set out above..."[39] This provision has since been updated with: "We may share your information with a parent, subsidiary, or other affiliate of our corporate group."

Pinterest

Pinterest's Privacy Policy states that user date are stored and transferred "**outside** your home country, including in the **United States**."[40]

LinkedIn

LinkedIn's Privacy Policy states that user data are stored "**outside** [users'] country" and that they transfer and process data "both inside and outside of the **United States**."[41]

Snapchat

Snap Inc.'s Privacy Policy states that they store, transfer, and process user data "**in the United States** and **other countries outside** of where [users] live."[42]

Twitter

Twitter's Privacy Policy states that the company stores user data in "**United States, Ireland and any other country where we operate**" so long as it is allowed by the country's laws of their users.[43]

Where do social media platforms store and transfer the personal data of its Canadian users?

Facebook
Facebook states that they own and operate their own data centres in the U.S., Europe and Asia.[44]

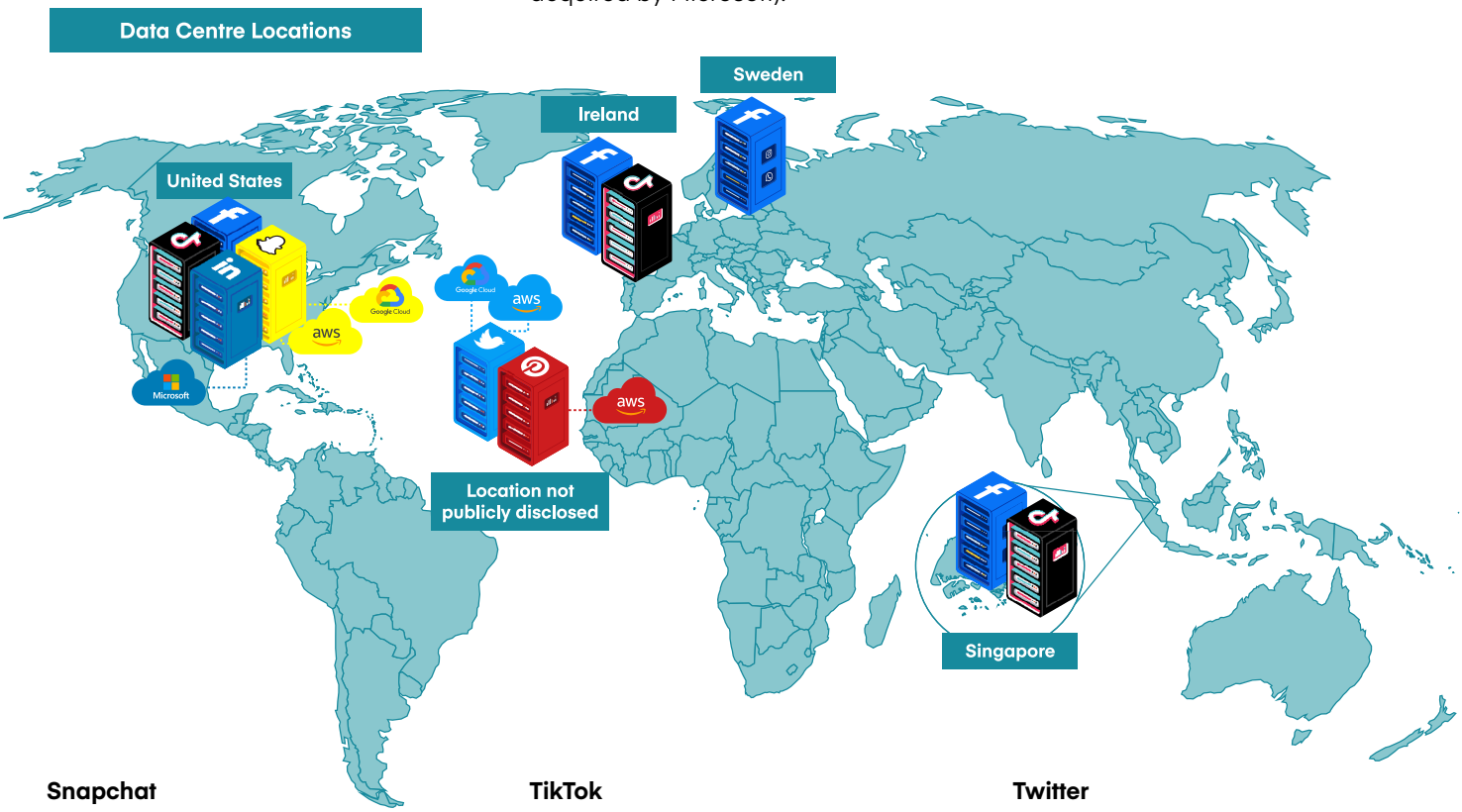
Data centre websites and blogs report that Facebook stores and transfers its data in the U.S., Sweden, Ireland and possibly Singapore.[45]

LinkedIn
LinkedIn states that it currently stores its members' information in the U.S.[46]

In 2019, LinkedIn disclosed that it used to run its own data centres in the U.S. and Singapore, but would now use cloud services provided by Microsoft Azure (after being acquired by Microsoft).[47]

Pinterest
Pinterest has not publicly disclosed where its data centres are located.

In 2017, Pinterest agreed to a deal with Amazon Web Services to host a "substantial majority" of its data. Amazon has data servers all over the world, including in Montréal, Québec.[48, 49]



Snapchat
Snapchat states that it stores data in the U.S.[50]

In its 2017 IPO filing, the company disclosed that it used the cloud storage services of both Google Cloud and Amazon Web Services.[51] Both Amazon and Google operate in jurisdictions around the world, including in Montréal, Québec.[52]

TikTok
TikTok has publicly disclosed the existence of data centres in Singapore, the U.S.[53] and Ireland.[54]

Twitter
Twitter has not publicly disclosed where its data centres are located.

In 2018, Twitter announced that it would begin using the services of Google Cloud for some of its data storage.[55] Twitter provides a list of service providers, including Amazon Web Services and Google, that indicates they operate in the U.S.; but it's not clear if that refers to data storage exclusively in the U.S.[56]

Canadian Law on Data Sovereignty

Canadian policy-makers at the federal level and in several provinces across the country are currently deciding how they will modernize their private sector privacy laws. In this section, we provide an explanation of the current laws as they relate to data sovereignty in Canada.

Federal Law Regulating Private Sector

At the federal level, Canadians' social media personal data are generally regulated by the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[57] It is a unique piece of legislation because it contains a mixture of requirements as well as recommendations. Schedule 1 of PIPEDA consists of ten principles that reproduce guidelines drafted by an industry association in the early 1990s,[58] which outline how organizations should collect, transfer and process personal data of Canadians.[59] It authorizes the Office of the Privacy Commissioner of Canada (OPC) to investigate complaints of non-compliance, but only to issue non-binding recommendations; while the Federal Court of Canada is able to provide binding decisions and remedies for complainant-initiated investigations (not those initiated by the OPC).[60]

Regarding data sovereignty, PIPEDA **does not prohibit** organizations from transferring personal data to third parties or outside of Canada. However, the Act does state that organizations are "responsible" for the protection of personal information that is transferred for processing, regardless of location.[61] When organizations transfer personal information to a third party for processing, PIPEDA requires organizations to provide a "**comparable level of protection**" to the protection it would receive had the information stayed within the possession of the organization.[62] However, the term "comparable level of protection" is undefined in PIPEDA and has not yet been interpreted in court.

PIPEDA also requires personal information to be protected against unauthorized access by security safeguards appropriate to the sensitivity of the information.[63] Finally, as of 2018, organizations are also required to report security breaches of personal information "under its control" to the OPC and affected individuals; Facebook, for example, notified 600,000 Canadians of the Cambridge Analytica data breach.[64]

The Office of the Privacy Commissioner of Canada (OPC) began a public consultation in 2019 on its policy position on transferring data outside of Canada under PIPEDA.[65] It stated that its position had evolved and that doing so should require:

- Explicit consent for personal data to be transferred outside of Canada; and
- Alternative options, if any, be communicated for those who do not wish to have personal information transferred outside of Canada.

In September 2019, the OPC concluded its consultation and decided not to alter its position.[66] Instead, OPC's guidelines continue to **allow companies to decide where Canadians' personal data will be stored and transferred without explicit consent.**[67]

There are longstanding criticisms of PIPEDA. The OPC itself has called the legislation outdated and inadequate for data protection due to a lack of enforcement.[68] PIPEDA also enables organizations to largely self-regulate and set their own standards for data protection, due to weak oversight powers on transfers of personal data outside of Canada.[69]

Since PIPEDA was enacted nearly 20 years ago, the OPC has released only 21 publicly-available investigation findings or case summaries that examine the "comparable level of protection" for the transfer of data to third parties.[70] Neither the Federal Court nor the Federal Court of Appeal, which have jurisdiction over PIPEDA claims, have ruled to provide enforcement or remedy regarding comparable levels of protection. In the two decades since the enactment of Canada's current privacy law, there has not been a single fine or enforced remedy against companies transferring personal data outside of Canada with insufficient protection.

This reinforces the reality that PIPEDA comprises principles that sound excellent on paper while enabling organizations to evade regulatory compliance when it comes to safeguarding the security and privacy of personal data for Canadians. The **self-regulatory approach of PIPEDA** fundamentally jeopardizes the security, privacy and protection of personal data for users of social media platforms — whose data can currently be freely transferred both outside of Canada and to third parties without the knowledge and consent of Canadian social media users, and without meaningful limitation under Canadian privacy law.

The 2019 mandate letter for Canada's Minister of Innovation, Science and Industry committed, in collaboration with the Minister of Justice and Minister of Canadian Heritage, to "enhanced powers for the Privacy Commissioner, in order to establish a new set of online rights, including … the knowledge of how personal data is being used, including with a national advertising registry and the ability to withdraw consent for the sharing or sale of data; the ability to review and challenge the amount of personal data that a company or government has collected; [and] proactive data security requirements."

It also committed to "new regulations for large digital companies to better protect people's personal data and encourage greater competition in the digital marketplace."The letter called for a newly created Data Commissioner to oversee these regulations.[71]

These commitments to new protections and powers are welcome news, because PIPEDA as it currently stands therefore leaves social media personal data vulnerable to the surveillance of other countries. It also leaves this data vulnerable to the access, use, transfer and processing by malicious attackers.

Provincial Law Regulating Private Sector

PIPEDA does not apply to the private sector in Alberta, British Columbia or Québec; these provinces have enacted private sector laws that have been deemed substantially similar to PIPEDA through federal regulatory exemptions.[72] None of these laws currently requires the private sector to store personal data in Canada, provided that the organization ensures third parties to which the data are transferred continue to comply with the requirements of the law.

Alberta is the only province with private sector privacy law that has a specific notice requirement for personal data transferred to a third-party service provider and stored outside of Canada. It requires that the organization develop and follow policies and practices that "include information regarding the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur."[73] It also requires that individuals be notified of transfer outside of Canada, and be provided with information about how to obtain access to the organizations' policies and practices with respect to service providers outside Canada, as well as the name or title of a person who is able to answer questions on behalf of the organization.[74]

In June 2020, the Government of Québec introduced Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information,* making significant changes to data transfer requirements outside of Québec. The draft Bill currently does not require that organizations obtain individual consent for transfers to third-party service providers, but does require that they conduct a Privacy Impact Assessment prior to transferring personal information outside of Québec. The organization would be required to take into account the sensitivity of the data, the protection measures that would apply and the degree of equivalency to Québec of the jurisdiction's legal framework with respect to the protection of personal information. It further provides that the government will publish a list of jurisdictions considered equivalent, similar to the GDPR provisions. These provisions, if passed, will come into force one year after the date of assent.[75]

As such, there is the potential for a **lack of consistency** in the privacy rights afforded by PIPEDA and the provincial laws that have been deemed substantially similar to PIPEDA.[76] This may be exacerbated further as Québec moves forward with more explicit requirements around data localization, and the Province of Ontario considers implementing its own private sector privacy law explicitly seeking to address gaps in legislation like PIPEDA.[77]

Public Sector Data Law

Compared to private sector law, Canadian laws and policies regarding storage of data collected by governments or public institutions provide more stringent requirements. Following the enactment of the U.S. *PATRIOT Act*, which expanded the surveillance powers of U.S. intelligence and law enforcement agencies, both British Columbia and Nova Scotia amended provincial law requiring personal information in the control of public institutions to be stored only in Canada. Some provincial legislation also restricts transfers of personal health data held by the public sector outside of Canada or that province.[78]

Since 2017, Government of Canada policy has required that data storage within Canada (or federal premises abroad such as a diplomatic or consular mission) be "identified and evaluated as a principal delivery option" for all data in its control classified as Protected B, Protected C or Classified.[79] Protected B and C classifications include information that could cause serious or grave injury to an individual or organization if compromised, such as financial, medical and legal information, but do not include personally identifying information, such as name, address and Social Insurance Numbers, which are considered Protected A.[80] In the Government of Canada's Information Technology Strategic Plan, it described this data localization requirement as necessary to "ensure Canada's sovereign control over its data, departments and agencies."[81]

Canada's International Trade Agreements

Canada is a signatory to various trade agreements that shape the development of privacy law in the country and may limit the ability to require data localization. For example, both the new Canada-United States-Mexico Agreement (CUSMA) and the Trans-Pacific Partnership prohibit signatories from implementing limitations on the transfer of data between countries subject to the agreement, unless doing so is necessary to achieve a "legitimate public policy objective".[82] The CUSMA further prevents requirements for the private sector (excluding financial institutions) to "use or locate computing facilities in that Party's territory as a condition for conducting business in that territory." This could be used to challenge legal requirements for data storage in Canada.[83]

Global Approaches to Data Sovereignty

Unlike Canada, other jurisdictions around the world explicitly regulate the storage and transfer location of social media personal data. In this section, we provide a scan of the current approaches to data sovereignty in other jurisdictions.

European Union (GDPR)

The GDPR prohibits the transfer of personal data outside of the European Economic Area (EEA), which includes all EU countries in addition to Iceland, Liechtenstein and Norway, unless the transfer meets one of three conditions:[84]

1. The transfer is to a country that has been assessed by the EU Commission to have **adequate safeguards** for data projection, equivalent to those in the EU.[85] The list of countries deemed adequate is continuing to evolve, but currently includes Canada.[86] The Canadian adequacy decision from 2001 was specific to organizations subject to PIPEDA, which had been assumed to include the three provincial laws deemed substantially similar to PIPEDA. However, a surprising 2014 EU decision recommended against adequacy for Québec, which has created uncertainty about Alberta and British Columbia's adequacy as well;[87]

2. The transfer has **appropriate safeguards**, which currently include standard contractual clauses or legally-binding corporate rules that provide for enforceable data security and protection, and only on the condition that enforceable data subject rights and effective legal remedies for data subjects are available;[88] or

3. The data subject provides **explicit consent** for personal data to be transferred outside of the EEA, only after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.[89]

In July 2020, the Court of Justice of the European Union declared invalid the EU-U.S. agreement on adequacy, which is currently undergoing appeal. The judgment cited the U.S. *Foreign Intelligence and Surveillance Act* and presidential executive orders on surveillance as not meeting the minimum proportionality principles under EU law.[90]

China

Most Western social media platforms are blocked in China; however, Chinese law generally requires personal data to be stored in China, unless the data transfer receives a positive security assessment from a Chinese provincial government.[91]

India

Indian law requires that personal data related to financial transactions only be transferred to other jurisdictions with explicit consent and adequate levels of protection.[92] The law also provides the government with authority to require that certain 'critical' personal data be stored and processed only in India, but it has not exercised this authority for social media data.[93] In June 2020, India blocked TikTok, WeChat and many other Chinese mobile apps, citing national security concerns.[94]

Russia

Russian law requires that all personal data of Russian citizens be stored in Russia, and was recently amended to increase penalties for non-compliance.[95] If the platforms are unable to determine citizenship of the data subject, the Russian government recommends localizing data with Russian IP addresses.[96] Google and Apple reportedly comply with this requirement, while LinkedIn is blocked within Russia for non-compliance.[97] Twitter and Facebook were both fined in 2020 for non-compliance, and Russian lawmakers are reportedly considering banning Facebook and Instagram.[98]

South Korea

South Korean law requires companies to obtain explicit consent from data subjects for transborder data transfer, which includes providing information about the data recipients, their purposes, the period of retention and the specific data to be provided.[99]

Turkey

In July 2020, Turkey amended its law to require personal data to be stored in Turkey for social media platforms with more than one million daily users in Turkey.[100] Facebook and Google have reportedly started using Turkey-based servers as a result.[101]

United States of America

While the U.S. does not have data localization requirements, it has used federal authority to try and shape where American user data are stored. In May 2019, the U.S. Committee on Foreign Investment in the United States required China's Beijing Kunlun Tech Co. to divest its majority stake in the gay dating app Grindr, citing concerns that sensitive personal data could be misused for blackmail.[102] In August 2020, President Trump signed executive orders declaring TikTok and WeChat would be blocked in the U.S. after 45 days. The WeChat ban was put on hold by a U.S. judge citing potential violations of freedom of speech rights; while the TikTok ban was put on hold pending a potential restructuring that will have American company Oracle operate a data cloud in the U.S. separate from its Chinese parent.[103]

Vietnam

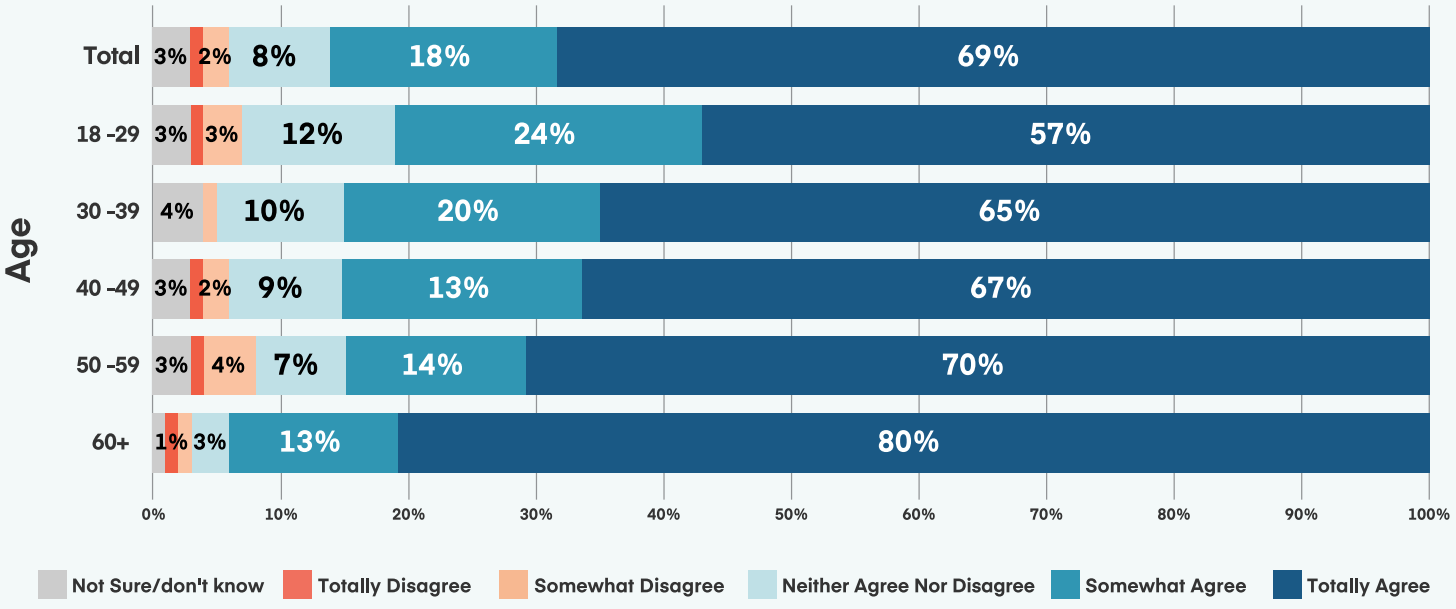
In 2019, Vietnam introduced requirements that online services establish a representative office in Vietnam and retain a copy of personal data in the country if the company is notified that its services have been used to commit violations of Vietnamese law and the company has not taken remedial measures to address the violations. The Vietnamese government notified Facebook that it was considered non-compliant by allowing users to post anti-government comments on the platform.[104]

Public Policy Options

Public Policy Question: How should Canadian privacy law protect the security and privacy of social media personal data stored outside of Canada?

To guide thinking about this policy question, it is important to understand the opinions of Canadians. A representative survey we conducted in May 2020 found that **Canadians overwhelmingly support the storage of Canadians' data in Canada** — with only 3% disagreement. Older Canadians felt even more strongly, with 93% agreement among those aged 60 or older. In interviews with Canadians, most cited concerns with government surveillance outside of Canada, principally from China and the United States. Those we spoke with who disagreed or were neutral on the issue were not any less concerned about data security or privacy but indicated weak trust with Canadian institutions, believing that storage in Canada could still be inappropriately surveilled or used.

"If companies that have my data want to operate in Canada, they should be required to keep Canadians' data within Canada and not allow access to other countries."



"I totally agree. We assume that if they are operating in Canada, they are keeping our data in Canada. There is so much on the news about China stealing information through applications that it makes you think about it."

"I don't think it makes a difference. No one is to trust, so it doesn't make a difference where my data is stored."

Our Framework

There are several policy options and considerations as private sector privacy law evolves that could better secure and protect social media personal data for people in Canada. In the following sections, we explore three options as the federal government modernizes PIPEDA regarding personal data transfers and storage outside of Canada. We examine the impacts of each option on three measures of analysis: its effect on the law; on social media companies; and finally on the privacy and data protection afforded to Canadians. Each option can be undertaken separately, or together with the others.

For the final and third measure of analysis focused on data protection, we would like to explicitly acknowledge that people who are racialized (particularly those who are Black and/or Indigenous), low-income, part of the LGBTQ+ community and other marginalized communities, are more likely to disproportionately benefit from any options that strengthen privacy and data protection for individuals. These populations continue to face longstanding threats to their privacy and disproportionate surveillance from law enforcement.[105] Digital technologies' abilities to match, categorize and sort individuals are often used in ways that magnify pre-existing discriminatory patterns and reflect long-standing social divisions that are deeply entangled with sexism, racism, homophobia, settler-colonialism and other intersecting oppressions.[106]

Option 1: (Actually) Require Comparable Levels of Protection

This option would strengthen PIPEDA to provide **precise requirements** and **enforcement**, to ensure that personal data receive a "comparable level of protection" as it would in Canada when they are transferred outside of the country.

This could mirror the GDPR model and the proposed new model in Québec by empowering the Office of the Privacy Commissioner of Canada (OPC) to assess the adequacy of the legal jurisdiction to which data are transferred, as well as the contractual obligations of the receiving organization.

Measure A: Impacts on Canadian Law

This option would require a more rigorous definition of the term "comparable level of protection" than currently exists within PIPEDA. It would also enable the OPC to assess and meaningfully enforce comparability. PIPEDA could be strengthened to provide for other jurisdictions to be deemed comparable, taking into consideration:

- The protection of rights and freedoms in law, particularly concerning the national security and law enforcement powers in the country where data are transferred or stored;
- The adequacy and meaningful enforcement of these protections; and
- Limitations or obligations regarding onward transfer to other countries.

Similar to the GDPR, PIPEDA could also provide for transfers to jurisdictions not deemed comparable through legally-binding and enforceable obligations, such as multinational corporate rules or contracts that protect and secure the rights of data subjects. These requirements could include:

- Appropriate security measures to protect against accidental or unlawful access, disclosure, modification or loss, such as encryption;
- Data use restrictions;
- Limitations on further transfer, including in the event of ownership change;
- Requirements that the contract is governed by the law of the data exporter, that the applicable law of the data importer does not prevent it from fulfilling these obligations, and requirements for prompt disclosure and termination if there is a change in this regard; and
- Enforcement mechanisms to assess compliance of the above.

Providing new authority to the OPC to conduct and enforce these assessments would also require additional investigative resources, as well as stronger investigative tools and financial penalties. The existing enforcement mechanisms within PIPEDA, including the inability to seek redress from OPC-initiated investigations or independently issue fines, are currently insufficient to protect Canadians. This could also include authority to enter into binding bi- or multilateral agreements with other jurisdictions to implement these protections, including for example with the European Union to maintain its adequacy decision under the GDPR.

Measure B: Impacts on Social Media Platforms

This option could have a potentially significant impact on social media platforms. Depending on how "comparable level of protection" is defined and operationalized, it could have a similar effect to that currently playing out between the EU and the U.S., where American platforms would be potentially barred from

storing or transferring Canadian user data to the U.S. if the country is deemed to have inadequate protections due to its surveillance powers. Changes to existing storage practices may have impacts on platforms' costs and revenues, as well as operations (e.g., content moderation, analytics).

However, this approach would still allow the platforms to remain relatively free to transfer personal data outside of Canada, so long as minimum conditions are met.

Measure C: Impacts on Data Protection for Canadians

Providing more precise requirements and enforcement to ensure transfers outside of Canada provide a comparable level of protection is much more likely to limit transfers to jurisdictions and organizations where Canadians' personal data are unlikely to be subjected to unauthorized access.

It is worth noting that critics of this approach point out that most cybersecurity vulnerabilities are exploited remotely or through insider threats, neither of which are addressed by the jurisdiction of the data, and that geographic constraints on cloud storage could improve threats actors' targeting.[107]

While this measure would not eliminate the risk of unauthorized data access or breach outside of Canada, it would be a significant step toward data sovereignty for Canadians' data.

Option 2: Require Explicit Consent for Transfer Outside of Canada

This option would strengthen PIPEDA to require social media platforms to **obtain explicit consent** from individuals for the transfer of their personal data to jurisdictions that do not provide comparable protection, and provide information regarding the specific data and countries involved in the transfer.

Under a consent model, individuals are provided with control over their personal data and can decide for themselves how to weigh the cost and benefits of the collection, use and disclosure of their information, and legitimize activities that would otherwise be illegitimate.[108]

Measure A: Impacts on Canadian Law

This option would require clarification in PIPEDA and the introduction of explicit requirements around transfers outside of Canada.

PIPEDA currently requires the knowledge and consent of the individual for the collection, use or disclosure of personal information. The current interpretation of this provision is that additional consent is not required when personal data are transferred to a third-party service provider or outside of Canada, so long as the data are being used for the purpose they were originally collected.

Measure B: Impacts on Social Media Platforms

This option would require that social media platforms collect explicit consent for transfer outside of Canada, and provide the specific personal data to be transferred and the countries where personal data could be stored.

This would likely require modifications to some platforms' privacy policies, particularly as they relate to transfers to third parties and affiliates. It could also lead to platforms providing exhaustive lists of all the countries in which data could be stored, to maintain flexibility for economic efficiency or innovation.

Measure C: Impacts on Data Protection for Canadians

This option would operationalize the principle that Canadians deserve to maintain control and decision-making over their personal data. The OPC stated in their 2019 consultation on this topic: "Where there is a meaningful risk that a residual risk of harm will materialize and will be significant, consent should be express, not implied."[109] The consent should also be freely given, specific, informed and unambiguous, ideally allowing individuals to use the service even if they do not consent to the data transfer.

Such an approach could act as a deterrent from platforms storing data in jurisdictions with poor reputations for human rights. It could also help to protect against the potential for changes in data storage and transfer practices after consent is provided, including in the event a platform's data are sold or merged. While we believe this option is an important step forward, it is unlikely to meaningfully change Canadians' digital privacy and security on its own. It would provide Canadians some additional information on the treatment of their personal data and may change the behaviour of some people. However, no amount of digital literacy and information can alter the market position of most of these platforms, and the take-it-or-leave-it consent model.

Online consent forms are often long and confusing. Scholars and experts argue that consent is being pushed beyond its capabilities in the social media era. In this context, consent does not provide people with meaningful control over their data. Too many entities are involved in complex and ongoing collection and use of personal data, such that even the most rational and well-informed person is unable to meaningfully weigh the costs and benefits.[110]

As such, additional public policy protections are needed regardless of individual consent.[111]

Option 3: Consider Special Protections for Sensitive Personal Data

This option would modernize Canadian privacy law to provide **special protections for sensitive personal data**. As an example, the law could require or provide regulation-making ability such that sensitive data collected by social media platforms be encrypted if transferred outside of Canada. That would involve a process to define this class of data. Defining a class of data as sensitive would provide organizations increased certainty regarding their obligation to safeguard against the unauthorized access or breach outside of Canada, even in countries deemed to provide a comparable level of protection. Biometric data, such as facial feature vectors, or private message content that can contain intimate medical, sexual and political information, could significantly jeopardize the safety and privacy of Canadians in the wrong hands.

Measure A: Impacts on Canadian Law

PIPEDA currently requires personal information to be protected by "security safeguards appropriate to the sensitivity of the information" and recommends that "more sensitive information should be safeguarded by a higher level of protection." This principle is elaborated in Schedule 1 as follows:
"Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive."[112]

These principles are desperately in need of modernization, clarity and greater enforcement. The GDPR, for example, provides extra protections for 'special category' data, which includes:

- Genetic, biometric and health data;
- Personal data revealing racial or ethnic origin, or religious beliefs;
- Personal data revealing political opinions or trade union membership; and
- Personal data concerning a person's sex life or sexual orientation.[113]

The GDPR generally prevents special category data from being processed by social media platforms without explicit consent, while also enabling member states to prohibit processing regardless of consent. Spain, for example, prohibits processing special category data, even with consent, if the principal purpose of the processing is to identify the data subject's ideology, trade union membership, religious beliefs, sexual orientation, or racial or ethnic origin.[114] This has, for example, prevented Facebook from targeting ads with users' religious and sexual orientation information collected from its new dating product.[115]

Measure B: Impacts on Social Media Platforms

This approach could require significant changes to the way that social media platforms operate in Canada.

Platforms could take the approach of localizing storage in Canada of either the sensitive data or the encryption keys to that data. Such a change may be challenged under the CUSMA, which generally prohibits Canada from requiring American businesses to have servers in Canada. It is uncertain whether a change in Canadian privacy law requiring that sensitive personal data be encrypted if transferred outside of Canada would meet this

test. This option could make it more difficult for individuals who travel in and out of Canada to access their personal data, and it is likely to impact social media platforms' costs, revenues, and operations (e.g., content moderation, analytics). In this way, it could favour larger companies that can operate at scale.

Platforms could also take the approach of implementing end-to-end encryption on sensitive data, such as private messages. End-to-end encryption means only the sender and receiver can open the data, and prevents the service provider or data storer from being able to decrypt the data. There is an ongoing debate in Canada and with its allies about access to end-to-end encrypted messages for the purposes of law enforcement and national security.[116] This policy debate and how best to protect the privacy and security of Canadians' private messages will be the subject of a forthcoming paper from the Cybersecure Policy Exchange. However, regardless of how sensitive data are encrypted or protected, we believe privacy and security protections for Canadians' most sensitive data should be within the control of Canadian decision-makers.

Measure C: Impacts on Data Protection for Canadians

If sensitive data are appropriately secured to prevent access outside of Canada, then there would be greater certainty that Canada's privacy and security laws would supersede in application before the laws of another country apply. The hope is that such requirements would better safeguard against the possibility of unauthorized or accidental access to Canadians' most sensitive information.

Conclusion

Canadian policy-makers at the federal and provincial levels face an immense challenge, and opportunity, as they modernize our privacy laws in the social media age. Privacy remains a fundamental right in Canada, even as the transfer of data across borders increasingly becomes the norm.[117] Foundational to our democracy is our ability to freely engage with each other, and to do so with trust and confidence that our privacy and security will be ensured. Increasingly, these engagements are taking place on digital platforms outside our borders.

Adequate protection of our personal data from unauthorized access, use and disclosure is a foundational legal principle enacted more than two decades ago. It is urgent that we modernize our laws to ensure that this principle and our privacy rights are upheld as we move increasing amounts of personal data to countries around the world. Canadians should have assurance that the jurisdictions where data are transferred protect and enforce their rights, transparent information to inform their decision, and confidence that their most sensitive data will never be compromised.

As jurisdictions around the world grapple with these challenges, many have rightly suggested there is a role for more coordinated international governance. Because platforms are global organizations and no one state can shift the structure of the social media platform economy, there are growing calls for greater international collaboration and coordination to regulate matters of data privacy, security, competition and content, similar to the post-war industrial rules that were developed to govern the financial markets, conflict prevention and so on.[118] The OECD's 2013 *Privacy Framework* and guidelines governing transborder flows of personal data are an example of existing efforts to this end.[119] There is debate about how such a platform governance model could be structured that is beyond the scope of this paper. However, we include this here to point out that Canada should continue to play a leadership role in coordinating such an approach that contributes toward greater data sovereignty, alongside the greater domestic protections and enforcement that we propose.

We put forward this discussion paper in the hope of advancing these objectives, in conversation with policy-makers, stakeholders, experts and civil society to enhance Canadians' trust and security online.

About the Authors

Yuan Stevens is the Policy Lead at the Cybersecure Policy Exchange and the Ryerson Leadership Lab. Yuan is an action-oriented researcher working at the intersections of law, policy and computer security. Her work equips society with the ability to understand and patch up harmful vulnerabilities in sociotechnical and legal systems. Passionate about building community, she is also a research affiliate at the Data & Society Research Institute and a research fellow at the Centre for Media, Technology & Democracy at McGill's School of Public Policy. She received her B.C.L./J.D. from McGill University in 2017, working as a research assistant for hacker expert Gabriella Coleman. She serves on the board of directors for Open Privacy Research Institute and previously worked at the Berkman Klein Center for Internet & Society at Harvard University.

Mohammed (Joe) Masoodi is a Policy Analyst at the Cybersecure Policy Exchange and the Ryerson Leadership Lab. Joe has been conducting research and policy analysis at the intersections of surveillance, digital technologies, security and human rights for over six years. He has conducted research at the Surveillance Studies Centre at Queen's University and the Canadian Forces College. He holds an MA in war studies from the Royal Military College of Canada; an MA in sociology from Queen's University; and has studied sociology as a PhD candidate from Queen's University, specializing in digital media, information and surveillance.

Sam Andrey is the Director of Policy & Research at the Ryerson Leadership Lab. Sam has led applied research and public policy development for the past decade, including the design, execution and knowledge mobilization of surveys, focus groups, interviews, randomized controlled trials and cross-sectional observational studies. He also teaches about public leadership and advocacy at Ryerson University and George Brown College. He previously served as Chief of Staff and Director of Policy to Ontario's Minister of Education, in the Ontario Public Service and in not-for-profit organizations advancing equity in education and student financial assistance reform. Sam has an Executive Certificate in Public Leadership from Harvard's John F. Kennedy School of Government and a BSc from the University of Waterloo.

Methodology

This paper was informed by:

- A literature review;
- A representative survey of 2,000 Canadians; and
- 20 interviews with Canadians regarding digital privacy and security.

Survey data cited in this report are from an anonymous survey conducted online by Pollara Strategic Insights with 2,000 Canadian residents aged 18 and older from May 14 to 22, 2020. A random sample of Canadian residents who have opted-in to the AskingCanadians panel were invited to complete the voluntary survey. The data were weighted by region, gender and age, based on the most recent Canadian census figures to ensure that the sample matched Canada's population. As a guideline, a probability sample of this size would yield results accurate to +/- 2 percentage points, 19 times out of 20 (95%). Totals may not sum or add to 100 due to rounding.

Table 1: Canadians' Perspectives on Data Localization

"Whether online services that operate in Canada, like Amazon, Facebook or Google, need to store the data they collect in Canada or outside of the country has been a topic of debate. To what extent do you agree with the following statement: 'If companies that have my data want to operate in Canada, they should be required to keep Canadians' data within Canada and not allow access to other countries.'"

	Total	Age					Gender		
		18-29	30-39	40-49	50-59	60+	Woman	Man	Other/Did not say
All Respondents (split sample)	1,000	206	172	160	198	264	512	484	4
Weighted Respondents	999	192	178	163	200	266	517	478	4*
Totally Agree	687	109	116	109	141	212	361	323	3
	69%	57%	65%	67%	70%	80%	70%	68%	75%
Somewhat Agree	176	47	35	30	29	35	87	90	0
	18%	24%	20%	19%	14%	13%	17%	19%	0%
Neither Agree nor Disagree	78	22	19	14	14	9	38	40	0
	8%	12%	10%	9%	7%	3%	7%	8%	0%
Somewhat Disagree	22	6	1	4	8	3	8	14	0
	2%	3%	1%	2%	4%	1%	1%	3%	0%
Totally Disagree	7	1	0	1	3	2	5	2	0
	1%	1%	0%	1%	1%	1%	1%	0%	0%
Not sure/Don't know	28	7	7	4	6	4	19	8	1
	3%	3%	4%	3%	3%	1%	4%	2%	25%

*very small base; ineligible for significance testing

Table 2: Canadians' Use of Social Media and Messaging Platforms

"Which online messaging or video call services or social media platforms have you used during the past two (2) months? (Select all that apply)"

	Total	Age					Gender		
		18-29	30-39	40-49	50-59	60+	Woman	Man	Other/Did not say
All Respondents	2,000	405	344	321	369	561	1,014	978	8
Weighted Respondents	2,000	380	351	334	371	564	1,025	968	8*
Online messaging or video calls	**1,589**	**321**	**309**	**264**	**278**	**417**	**826**	**756**	**6**
	79%	**85%**	**88%**	**79%**	**75%**	**74%**	**81%**	**78%**	**75%**
Facebook Messenger	1,102	259	219	166	181	276	610	488	3
	55%	68%	62%	50%	49%	49%	60%	50%	38%
WhatsApp	650	159	181	114	98	98	312	333	5
	33%	42%	52%	34%	26%	17%	30%	34%	63%
Instagram Direct Messages	330	151	83	34	26	36	206	123	1
	17%	40%	24%	10%	7%	6%	20%	13%	13%
Twitter Direct Messages	96	34	18	11	19	13	38	58	0
	5%	9%	5%	3%	5%	2%	4%	6%	0%
WeChat	74	22	15	17	9	10	33	40	1
	4%	6%	4%	5%	2%	2%	3%	4%	13%
Telegram	36	13	12	7	4	0	13	23	0
	2%	3%	3%	2%	1%	0%	1%	2%	0%
Signal	19	2	6	4	6	0	5	14	0
	1%	1%	2%	1%	2%	0%	0%	1%	0%
Social media	**1,530**	**337**	**296**	**259**	**275**	**362**	**806**	**719**	**5**
	76%	**89%**	**84%**	**78%**	**74%**	**64%**	**79%**	**74%**	**62%**
Facebook	1,381	299	265	236	245	336	742	636	3
	69%	79%	75%	71%	66%	60%	72%	66%	38%
Instagram	836	273	210	140	104	108	475	357	3
	42%	72%	60%	42%	28%	19%	46%	37%	38%
LinkedIn	542	142	114	100	102	85	231	308	3
	27%	37%	32%	30%	27%	15%	23%	32%	38%
Twitter	500	132	105	88	86	89	213	286	1
	25%	35%	30%	26%	23%	16%	21%	30%	13%
Pinterest	425	115	75	54	84	97	300	125	0
	21%	30%	21%	16%	23%	17%	29%	13%	0%
Snapchat	339	201	73	23	27	15	192	147	0
	17%	53%	21%	7%	7%	3%	19%	15%	0%
Reddit	239	109	59	38	26	8	81	157	1
	12%	29%	17%	11%	7%	1%	8%	16%	13%
TikTok	190	83	39	29	27	13	116	75	0
	10%	22%	11%	9%	7%	2%	11%	8%	0%

References

[1]Schrems, M. (n.d.). Objectives of "europe-v-facebook.org". Retrieved from: http://europe-v-facebook.org/EN/Objectives/objectives.html

Schrems v. Facebook Ireland Ltd, 2016 Data Protection Commissioner at paras 17-18.

[2]Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems,* 2020 High Court (Ireland).

Schrems v. Facebook Ireland Ltd, 2016 Data Protection Commissioner at paras 17-18.

[3]Bender, D. (2016, November 8). The Demise of Safe Harbor and Rise of Privacy Shield: How Can Personal Information Now Be Exported from the EU to the United States?. *LexisNexis*. Retrieved from: https://www.lexisnexis.com/lexis-practical-guidance/the-journal/b/pa/posts/the-demise-of-safe-harbor-and-rise-of-privacy-shield-how-can-personal-information-now-be-exported-from-the-eu-to-the-united-states

International Trade Administration. (n.d.) How to Join Privacy Shield (part 1). Retrieved from: https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1

Thomson Reuters (n.d.) US-EU Safe Harbor Framework. *Thomson Reuters Practical Law*. Retrieved from: https://ca.practicallaw.thomsonreuters.com/2-501-8616?transitionType=Default&contextData=(sc.Default)&firstPage=true

[4]Alley, A. (2020, September 11) Ireland to order Facebook to halt data transfers from EU to US. *Data Center Dynamics*. Retrieved from: https://www.datacenterdynamics.com/en/news/ireland-order-facebook-halt-data-transfers-out-eu-irish-data-protection-commission/

Baskett, N. (2020) The Court of Justice of the European Union ruling in Data Protection Commissioner v Facebook Ireland and Maximillian Schrems Judgment in Case C-311/18. *Data Protection & Privacy*, 3(4), 460-462. Retrieved from: https://hstalks.com/article/5884/the-court-of-justice-of-the-european-union-ruling-/

Weckler, A. (2020, September 9). Irish data regulator orders Facebook to stop sending personal data to the US. *Independent.* Retrieved from: https://www.independent.ie/business/technology/irish-data-regulator-orders-facebook-to-stop-sending-personal-data-to-the-us-39518775.html

[5]The White House, United States Government. (2020, August 6). *Executive Order on Addressing the Threat Posed by TikTok*. Retrieved from: https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

[6]Swanson, A., McCabe, D., & Griffith, E. (2020, September 19). Trump Approves Deal Between Oracle and TikTok. *New York Times.* Retrieved from: https://www.nytimes.com/2020/09/19/technology/trump-oracle-and-tiktok.html

[7]Abi-Habib, M. (2020, June 29). India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat. *New York Times*. Retrieved from: https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html

[8]Bodoni, S. (2020, June 10). TikTok Faces Scrutiny From EU Watchdogs Over Data Practices. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2020-06-10/tiktok-faces-scrutiny-from-eu-watchdogs-over-privacy-practices?sref=QqWIvTvt

[9]Hong v. Bytedance, Inc., 2019 United States District Court Northern District of California.

[10]Ryerson Leadership Lab. (2019, September). Rebuilding the Public Square. *Ryerson University.* Retrieved from: https://www.ryersonleadlab.com/rebuilding-the-public-square

[11]Finlay, C., Bardeesy, K. & Su, Y. (2020, July 9). Advancing a Cybersecure Canada: Introducing the Cybersecure Policy Exchange. *Cybersecure Policy Exchange*. Retrieved from: https://www.cybersecurepolicy.ca/agenda

[12]Ryerson Leadership Lab (2019)

[13]Conger, K. & Popper, N. (2020, July 31). Florida Teenager Is Charged as 'Mastermind' of Twitter Hack. *New York Times.* Retrieved from: https://www.nytimes.com/2020/07/31/technology/twitter-hack-arrest.html

Franceschi-Bicchierai, L. (2016, May 18). Another Day, Another Hack: 117 Million LinkedIn Emails and Passwords. *Vice*. Retrieved from: https://www.vice.com/en/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password

Hollister, S. (2019, May 23). Snapchat: Your latest reminder anyone a company hires could theoretically breach your privacy. *The Verge*. Retrieved from: https://www.theverge.com/2019/4/24/18514500/company-employee-hiring-privacy-breach-personal-data-theft

Winder, D. (2020, August 19). 235 Million Instagram, TikTok And YouTube User Profiles Exposed In Massive Data Leak. *Forbes*. Retrieved from: https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=666d9ecc1111

[14]Petrov, C. (2020, August 30). 50 Data Breach Statistics to Help You Run a Safer Enterprise in 2020. *TechJury.* Retrieved from: https://techjury.net/blog/data-breach-statistics/#gref

Savoie, A., & Thibodeau, M. O. (2019). The Inception of an International Grand Committee. *Canadian Parliamentary Review,* 42(3). Retrieved from: https://www.questia.com/library/journal/1G1-608615241/the-inception-of-an-international-grand-committee

[15]Wiener-Bronner, D. (2018, March 21). Mark Zuckerberg has regrets: 'I'm really sorry that this happened'. *CNN*. Retrieved from: https://money.cnn.com/2018/03/21/technology/mark-zuckerberg-apology/index.html

[16]Tobin, M. (2020, August 18). Beijing's shadow falls across Hong Kong. *Rest of World*. Retrieved from: https://restofworld.org/2020/the-great-firewall-comes-for-hong-kong/

[17]Peterson, A. (2015, March 26). Bankrupt RadioShack wants to sell off user data. But the bigger risk is if a Facebook or Google goes bust. *Washington Post*. Retrieved from: https://www.washingtonpost.com/news/the-switch/wp/2015/03/26/bankrupt-radioshack-wants-to-sell-off-user-data-but-the-bigger-risk-is-if-a-facebook-or-google-goes-bust/

[18]Fraser, E. (2016). Data Localisation and the Balkanisation of the Internet. *Scripted*, 13(3).

[19]Boyd, D.M. and Ellison, N.B. (2007). Social Network Sites: Definition, History, and Scholarship. *Computer-Mediated Communication*, 13(1), 210-230. Retrieved from: https://academic.oup.com/jcmc/article/13/1/210/4583062

Scott, P.R. and Jacka, J. M. (2011) *Auditing Social Media*: A Governance and Risk Guide. Wiley Publishing.

[20]Office of the Privacy Commissioner of Canada. (2013). *Personal Information*. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/

[21]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or GDPR) Art. 4(1)

[22]Franssen, M., Lokhorst, G.-J., & van de Poel, I. (2018). Philosophy of Technology. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Stanford University. Retrieved from: https://plato.stanford.edu/entries/technology/#DeveEthiTech

Lakoff, G., & Johnson, M. (2003). *Metaphors we live by. University of Chicago Press*.

[23]Curry, S. (2007). Sovereignty and jurisdiction. In D.S. Clark (Ed.)., *Encyclopedia of Law & Society: American and Global Perspectives* (pp. 1423-1424). Thousand Oaks, CA.

De Filippi, P. & McCarthy, S. (2012). Cloud Computing: Centralization and Data Sovereignty. *European Journal of Law and Technology*, 3(2).

Peterson, Z.N.J., Gondree, M. & Beverly, R. (2011). A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud. *Paper presented at the 3rd USENIX Workshop on Hot Topics in Cloud Computing*. Retrieved from: https://www.usenix.org/legacy/event/hotcloud11/tech/final_files/Peterson.pdf

[24]Latour, J. (2018, January 24). Data sovereignty: What you need to know and why you should care. *Cira*. Retrieved from: https://www.cira.ca/blog/state-internet/data-sovereignty-what-you-need-know-and-why-you-should-care

[25]See e.g. the General Data Protection Regulation, Art. 4(1).

[26]See e.g. from the General Data Protection Regulation, Art. 4(2).

[27]David Young Law. (2019). Transfers for processing under PIPEDA: a transfer is a use, not a disclosure. *David Young Law*. Retrieved from: https://davidyounglaw.ca/compliance-bulletins/transfers-for-processing-under-pipeda-a-transfer-is-a-use-not-a-disclosure/

Kermani, N., McAlister, M., Ruby, P. (2019, April 15). Privacy Commissioner Reverses its Position on Cross-Border Transfers of Personal Information. *Goodmans LLP*. Retrieved from: https://www.goodmans.ca/Doc/Privacy_Commissioner_Reverses_its_Position_on_Cross_Border_Transfers_of_Personal_Information

[28]Peterson, Z.N.J., Gondree, M. & Beverly, R. (2011); Filippi, P. D., & McCarthy, S. (2012).

[29]Mell, P. M., & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[30]Office of the Privacy Commissioner of Canada. (2019, June 11). *Consultation on transborder dataflows*. Retrieved from: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-transborder-dataflows/

Sargsyan, T. (2016). Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security. *International Journal of Communication*, 10.

[31]Pernot-Leplay, E. (2020). China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU? *Penn State Journal of Law & International Affairs*, 8(1).

[32]Wallace. C.E. (2020, March 4). Dangerous partners: big tech and Beijing. *Federal Bureau of Investigation*. Retrieved from: https://www.fbi.gov/news/testimony/dangerous-partners-big-tech-and-beijing

[33]LinkedIn. (2020, August 11). Cross-Border Data Transfers. Retrieved from: https://www.linkedin.com/legal/privacy-policy#other_information:~:text=5.2.%20Cross%2DBorder%20Data%20Transfers

[34]Pinterest. (2020, September 2). Pinterest Privacy Policy. Retrieved from: https://policy.pinterest.com/en/privacy-policy

[35]Twitter. (2020, June 18). Twitter Privacy Policy. Retrieved from: https://twitter.com/en/privacy

[36]Facebook. (2020, August 21). Data Policy. Retrieved from: https://www.facebook.com/full_data_use_policy

[37]Zuckerberg, M. (2020, October 19). A Privacy-Focused Vision for Social Networking. *Facebook*. Retrieved from: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

[38]TikTok. (2020, January 1). Legal: Privacy Policy. Retrieved from: https://www.tiktok.com/legal/privacy-policy?lang=en

[39]Carroll, D. (2019). Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?. *Quartz*. Retrieved from: https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/

[40]Pinterest. (2020).

[41]LinkedIn. (2020, August 11). Privacy Policy. Retrieved from: https://www.linkedin.com/legal/privacy-policy

[42]Snap Inc. (2020, September 14). Privacy Policy. Retrieved from: https://www.snap.com/en-US/privacy/privacy-policy

[43]Twitter. (2020).

[44]Facebook. (2016, September 20). Facebook Infrastructure: Inside Data Center Strategy and Development. *Facebook*. Retrieved from: https://www.facebook.com/careers/life/facebook-infrastructure-inside-data-center-strategy-and-development

[45]Baxtel. (n.d.) Facebook Data Center News. *Baxtel*. Retrieved from: https://baxtel.com/data-centers/facebook/news

Data Center Knowledge. (2010, September 27). *The Facebook Data Center FAQ*. Data Center Knowledge. Retrieved from: https://www.datacenterknowledge.com/data-center-faqs/facebook-data-center-faq

[46]LinkedIn. (2020). EU, EEA, and Swiss Data Transfers. Retrieved from: https://www.linkedin.com/help/linkedin/answer/62533?trk=microsites-frontend_legal_privacy-policy&lang=en

[47]Protalinski, E. (2019, July 23). LinkedIn is migrating to Microsoft Azure. *VentureBeat*. Retrieved from: https://venturebeat.com/2019/07/23/linkedin-is-migrating-to-microsoft-azure/

[48]Krazit, T. (2019). Pinterest cut a deal with Amazon Web Services that requires it to spend $750 million with the cloud leader by 2023. *GeekWire*. Retrieved from: https://www.geekwire.com/2019/pinterest-cut-deal-amazon-web-services-requires-spend-750-million-cloud-leader-2023/

[49]Poccia, D. (2020, March 30). Now Open: Third Availability Zone in the AWS Canada (Central) Region. *Amazon*. Retrieved from: https://aws.amazon.com/blogs/aws/now-open-third-availability-zone-in-the-aws-canada-central-region/

[50]Snap Inc. (n.d.). Snapchat Support. Retrieved from: https://support.snapchat.com/en-US/a/snapchat-service-providers

[51]Levy, A. (2017, February 9). Snap's cloud bill this year will be higher than its total revenue for 2016. *CNBC*. Retrieved from: https://www.cnbc.com/2017/02/09/snap-cloud-bill-aws-google-cloud-higher-than-2016-revenue.html

[52]Google. (n.d.). Cloud locations. Retrieved from: https://cloud.google.com/about/locations

[53]Pappas, V. (2019, November 5). Explaining TikTok's approach in the US. *TikTok*. Retrieved from: https://newsroom.tiktok.com/en-us/explaining-tiktoks-approach-in-the-us

[54]Cloutier, R. (2020, August 6). Establishing a new European data centre in Ireland. *TikTok*. Retrieved from: https://newsroom.tiktok.com/en-gb/establishing-a-new-european-data-centre-in-ireland

[55]Agrawal. P. (2018, May 3). A new collaboration with Google Cloud. *Twitter*. Retrieved from: https://blog.twitter.com/engineering/en_us/topics/infrastructure/2018/a-new-collaboration-with-google-cloud.html

[56]Twitter. (n.d.). Our Service Partners. Retrieved from: https://privacy.twitter.com/en/subprocessors

[57]Office of the Privacy Commissioner of Canada. (2010). Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing. Retrieved from: https://www.priv.gc.ca/media/1961/report_201105_e.pdf

[58]*Englander v. Telus Communications Inc.,* 2004 Federal Court of Appeal at para 8

[59]*Personal Information Protection and Electronic Documents Act,* RSC 2000, Schedule 1

[60]Innovation, Science and Economic Development Canada. (2019, May 21). *Strengthening Privacy for the Digital Age*. Retrieved from https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

[61]*Personal Information Protection and Electronic Documents Act*, RSC 2000, Schedule 1 PIPEDA, Principle 1

[62]*Personal Information Protection and Electronic Documents Act*, RSC 2000, Schedule 1, 4.1.3

[63]*Personal Information Protection and Electronic Documents Act*, RSC 2000, Schedule 1, 4.7

[64]Global News. (2018, April 4). Over 600,000 Canadians' Facebook data shared with Cambridge Analytica in data leak. *Global News*. Retrieved from: https://globalnews.ca/news/4123259/facebook-data-breach/

Personal Information Protection and Electronic Documents Act, RSC 2000, s. 10.1(1)

[65]Office of the Privacy Commissioner of Canada. (2009, January 27). Guidelines for processing personal data across borders. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/

[66]Office of the Privacy Commissioner of Canada. (2019, September 23). *Commissioner concludes consultation of transfers for processing*. Retrieved from: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/

[67]Office of the Privacy Commissioner of Canada. (2009, January 27).

[68]Office of the Privacy Commissioner of Canada. (2013, May). The Case for Reforming the *Personal Information Protection and Electronic Documents Act*. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/

Office of the Privacy Commissioner of Canada. (2018, September 27). *Privacy Commissioner denounces slow progress on fixing outdated privacy laws*. Retrieved from: https://priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180927/?wbdisable=true

Tousaw, K. (2006, March). Securing compliance, protecting privacy: The PIPEDA enforcement evaluation research project. *B.C. Civil Liberties Association*. Retrieved from: https://bccla.org/wp-content/uploads/2012/03/2006-BCCLA-Policy-Securing-Compliance.pdf

Scassa, T. (2018, June 7). Reforms to the Personal Information Protection and Electronics Documents Act must give the privacy commissioner real enforcement powers. *Policy Options*. Retrieved from: https://policyoptions.irpp.org/magazines/june-2018/enforcement-powers-key-pipeda-reform/

[69]Note that the standard of proof for PIPEDA's breach reporting regulation refers to a "real risk of significant harm"; see: *Personal Information Protection and Electronic Documents Act,* RSC 2000, s. 10.1(1)

[70]Office of the Privacy Commissioner of Canada. (2020, April 22). *Investigations into businesses*. Retrieved from: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/?t=comparable+level+of+protection&Page=1

[71]Prime Minister's Office. (2019, December 13). Minister of Innovation, Science and Industry Mandate Letter. Retrieved from: https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-innovation-science-and-industry-mandate-letter

[72]Office of the Privacy Commissioner of Canada. (2020, May). *Provincial laws that may apply instead of PIPEDA*. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/

[73]*Personal Information Protection Act*, SA 2003, s. 6(2)

[74]*Personal Information Protection Act*, SA 2003, s. 13.1

[75]*An Act to modernize legislative provisions as regards the protection of personal information,* Assemblée nationale du Québec, 2020

BLG. (2020, June 15). Proposed amendments to Quebec privacy law: Impact and for businesses. *BLG Law*. Retrieved from: https://www.blg.com/en/insights/2020/06/proposed-amendments-to-quebec-privacy-law-impact-for-businesses

[76]Michaluk, D.J. (2020, August 25). Ontario signals the coming of commercial privacy legislation. *Lexology*. Retrieved from: https://www.lexology.com/library/detail.aspx?g=7b148b58-a17b-4765-9424-58d020489b09

Power, M. (2015, January 19). Federal private sector: Not just one regulator anymore? *Michael Power.* Retrieved from: http://michaelpower.ca/2015/01/federal-private-sector-not-just-the-opc-anymore/

[77]McMillan LLP (2014, November 3). Canadian Telcos and banks subject to the Quebec privacy law. *McMillan.* Retrieved from: https://www.mondaq.com/canada/privacy-protection/351346/canadian-telcos-and-banks-subject-to-the-quebec-privacy-law

Ministry of Government and Consumer Services. (2020, August 13). Consultation: strengthening privacy protections in Ontario. *Government of Ontario.* Retrieved from: https://www.ontario.ca/page/consultation-strengthening-privacy-protections-ontario

[78]*Freedom of Information and Protection of Privacy Amendment Act,* SBC 2004

Nova Scotia Personal Information International Disclosure Protection Act, SNS 2006

Personal Health Information Privacy and Access Act, SNB 2009

Personal Health Information Protection Act, SO 2004

[79]Government of Canada. (2019, August 2). Directive on Service and Digital. Retrieved from: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601

[80]Department of Justice, Canada. (2016, September 6). Department of Justice Guidelines on Security for Domestic Legal Agents: Protected Information and Assets. *Government of Canada.* Retrieved from: https://www.justice.gc.ca/eng/abt-apd/la-man/security-securite/a.html

Government of Canada. (2020, June 16). Levels of security. Retrieved from: https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html

[81]Treasury Board of Canada Secretariat. (2017). Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021. *Government of Canada.* Retrieved from: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html

[82]Canada-United States-Mexico Agreement, s. 19.11.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership, s. 14.11.

[83]Canada-United States-Mexico Agreement, s. 19.12.

Jarvie, M. (2020, June). Canada: Cross-border transfers and data localisation after the USMCA. *OneTrust DataGuidance.* Retrieved from: https://www.dataguidance.com/opinion/canada-cross-border-transfers-and-data-localisation-after-usmca

Geist, M. (2018, October 10). How Canada Surrendered Policy Flexibility for Data Localization Rules in the USMCA. Retrieved from: https://www.michaelgeist.ca/2018/10/how-canada-surrendered-policy-flexibility-for-data-localization-rules-in-the-usmca/

[84]General Data Protection Regulation, Chapter 5.

[85]General Data Protection Regulation, Art. 45.

[86]Chander, A. (Forthcoming 2020) Is data localization a solution for Schrems II? *Journal of International Economic Law.* Retrieved from: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3318&context=facpub

Others include Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

[87]Bennett, C.J. (2016, August 8). Is Canada still 'adequate' under the new European general data protection regulation. Retrieved from: https://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-new-general-data-protection-regulation/

McCarthy Tetrault. (2020, June 19).Bill 64: An overhaul of Quebec's privacy law regime: implications for businesses. Retrieved from: https://www.mccarthy.ca/en/insights/blogs/techlex/bill-64-overhaul-quebecs-privacy-law-regime-implications-business

Uzan-Naulin, J. (2020, August 18).Bill 64 Mirroring the GDPR?. *Mondaq*. Retrieved from: https://www.mondaq.com/canada/privacy-protection/977004/bill-64-mirroring-the-gdpr

[88]General Data Protection Regulation, Art. 46.

[89]General Data Protection Regulation, Art. 49.

[90]Schwartz, P., & Peifer, K. (2019). Data localization under the CLOUD Act and the GDPR. *Computer Law Review International.* Retrieved from: https://paulschwartz.net/wp-content/uploads/2020/08/Schwartz-Peifer-Data-Localization-CRi-2019-1.pdf

[91]Albrecht, D. (2020, February 27). Measures on security assessment of cross-border transfer of personal information. *IP-Insider.* Retrieved from: http://www.youripinsider.eu/measures-security-assessment-cross-border-transfer-personal-information-2019-draft/

Leskin, P. (2019, October 10). Here are all the major US tech companies blocked behind China's 'Great Firewall'. *Business Insider.* Retrieved from: https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5

Zhang, D. (2020, July). China: Data localization requirements. *OneTrust DataGuidance.* Retrieved from: https://www.dataguidance.com/opinion/china-data-localisation-requirements

Selby, J. (2017). Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology*, 25(3), pp 213–232.

[92]Rishab, B. and Parsheera, S. (2018). Data Localisation in India: Questioning the Means and Ends. NIPFP Working Paper No. 242.

[93]Basu, A. (2020, January 10). The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam. *The Diplomat*. Retrieved from: https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/

Bryant, J. (2019, December 17). What you should know about India's forward-moving privacy bill. *International Association of Privacy Professionals.* Retrieved from: https://iapp.org/news/a/indias-data-privacy-bill-under-committee-review/

[94]Abi-Habib (2020)

[95]Bauer, M., Hosuk, L., Van der Marel, E. and Vershelde, B. (2015). Data localization in Russia: A self-imposed sanction. *ECIPE Policy Brief*. Retrieved from: http://hdl.handle.net/10419/174795

[96]Rumyantsev, S. (2019, December 10). Russia sets $280,000 fine for breaching data localization law. *Gorodissky & Partners.* Retrieved from: https://www.gorodissky.com/publications/articles/russia-sets-280-000-fine-for-breaching-data-localization-law/

[97]Blagov, S. (2015, December 22). Apple, Google meeting Russia data-localization rules. *Bloomberg Law.* Retrieved from: https://news.bloomberglaw.com/tech-and-telecom-law/apple-google-meeting-russia-data-localization-rules

Lunden, I. (2016, November 17). LinkedIn is now officially blocked in Russia. *TechCrunch*. Retrieved from: https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/?_ga=2.209502994.1466512653.1602796747-1497040547.1601820473

[98]Associated Press. (2020, February 13). Twitter, Facebook fined for not moving user data to Russia. Retrieved from: https://apnews.com/article/a4fa655e946b9441b6e68ee3592a8f27

Doffman, Z. (2019, September 13). Facebook, Instagram And YouTube Will Now Be Banned, Russians Warned. *Forbes*. Retrieved from: https://www.forbes.com/sites/zakdoffman/2019/09/13/putin-now-plans-100-facebook-instagram-and-youtube-bans-russians-warned/#223718c457ff

[99]*Personal Information Protection Act,* South Korea Act No.16930, Article 39-12, amended 2020

[100]Okumus, B.Y., Savuran., S.B., and Talay, Y.U. (2020, August 12). Amendments to the law No: 5651 concerning social media. *Mondaq*. Retrieved from: https://www.mondaq.com/turkey/social-media/975654/amendments-to-the-law-no-5651-concerning-social-media

[101]Ozturan, G. (2020). Turkey's 'data localization bill' in the aims of total control over social media. *Dokuz 8 Haber.* Retrieved from: https://dokuz8haber.net/english/science-technology/turkey-data-localization-bill-in-aims-of-total-control-over-social-media/

[102]Peters, J. (2020, May 6). Grindr has been sold by its Chinese owner after the US expressed security concerns. *The Verge*. Retrieved from https://www.theverge.com/2020/3/6/21168079/grindr-sold-chinese-owner-us-cfius-security-concerns-kunlun-lgbtq

[103]Swanson (2020)

[104]CNBC. (2019, Jan 9). Vietnam says Facebook violated controversial cybersecurity law. Retrieved from: https://www.cnbc.com/2019/01/09/vietnam-says-facebook-violated-controversial-cybersecurity-law.html

Vishwakarma, N. (2019, October 21). Vietnam plans to narrow data localization requirements under its cybersecurity law. *Medianama*. Retrieved from: https://www.medianama.com/2019/10/223-data-localisation-vietnam/

[105]Gandy, O. (1993). *The Panoptic Sort: a political economy of personal information.* Routledge: London.

Kenyon, M. (2020, September 1). Algorithmic policing in Canada explained. *CitizenLab*. Retrieved from: https://citizenlab.ca/2020/09/algorithmic-policing-in-canada-explained/

[106]Bailey, J., Burkell, J., and Steeves, V. (2020, August 24). AI technologies, like police facial recognition, discriminate against people of colour. *The Conversation*. Retrieved from: https://theconversation.com/ai-technologies-like-police-facial-recognition-discriminate-against-people-of-colour-143227

[107]Amazon. (2020, August). Data Residency: *AWS Policy Perspectives*. Retrieved from: https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

[108]Solove, D. (2013). Introduction: privacy, self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880-1903.

[109]Office of the Privacy Commissioner of Canada. (2019, June 11).

[110]Goold, B. (2009). Surveillance and the political value of privacy. Amsterdam Law Forum, 1(4). Retrieved from: https://commons.allard.ubc.ca/cgi/viewcontent.cgi?article=1153&context=fac_pubs

[111]Solove (2013)

[112]*Personal Information Protection and Electronic Documents Act,* RSC 2000, Schedule 1, 4.3.4.

[113]General Data Protection Regulation, Art. 9(1).

[114]Two Birds. (2020). Special rules for special categories of data. *Bird and Bird*. Retrieved from: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/special-categories-of-personal-data

[115]Lomas, N. (2020, October 22). Facebook Dating launches in Europe after 9 month delay over privacy concerns. *TechCrunch.* Retrieved from: https://techcrunch.com/2020/10/22/facebook-dating-launches-in-europe-after-9-month-delay-over-privacy-concerns/

[116]U.S. Department of Justice. (2020, October 11). International Statement: End-To-End Encryption and Public Safety. Retrieved from: https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

[117]Health Canada. (2008, August). Privacy: a fundamental right in Canada. Government of Canada. Retrieved from: https://www.canada.ca/en/health-canada/services/environmental-workplace-health/reports-publications/occupational-health-safety/privacy-fundamental-right-canada-national-dosimetry-services.html

[118]Etlinger, S. (2019, October 28). What's so difficult about social media platform governance? *CIGI Online.* Retrieved from: https://www.cigionline.org/articles/whats-so-difficult-about-social-media-platform-governance

[119]Organisation for Economic Co-Operation and Development. (2013). *The OECD Privacy Framework.* Retrieved from: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf


cybersecure
policy
exchange
Powered by
RBC