CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

IMPLEMENTING DATA PORTABILITY: LESSONS FOR A MADE-IN-CANADA APPROACH

21-1879

ABOUT CPA CANADA

Chartered Professional Accountants of Canada (CPA Canada) works collaboratively with the provincial, territorial and Bermudian CPA bodies, as it represents the Canadian accounting profession, both nationally and internationally. This collaboration allows the Canadian profession to champion best practices that benefit business and society, as well as prepare its members for an ever-evolving operating environment featuring unprecedented change. Representing more than 220,000 members, CPA Canada is one of the largest national accounting bodies worldwide. **cpacanada.ca**

Electronic access to this report can be obtained at **cpacanada.ca**

Table of Contents

Introduction

As the digital economy continues to grow, concerns over individuals' privacy rights are leading countries worldwide to tighten up their data privacy laws and give consumers more control over their personal data. At the same time, advancing technology and ever-growing pools of consumer data are opening up new possibilities for innovative businesses.

In Canada, the federal government has tabled privacy reform legislation that aims to modernize and strengthen the existing Personal Information Protection and Electronic Documents Act (PIPEDA). Bill C-11, the Digital Charter Implementation Act, proposes to replace PIPEDA with a new Consumer Privacy Protection Act (CPPA) that would give Canadian consumers more power over their personal data held by organizations. The new legislation includes new rights for individuals to request access, correction or deletion of their personal data (often referred to as "data subject rights").

The rights also include a new data mobility right that will allow Canadian consumers to ask organizations to transfer their personal data to another organization so it can be reused. The right is expected to enhance consumer choice and stimulate business innovation by giving individuals more control over the information they impart to businesses. Data mobility is intended to help consumers avoid being locked into a relationship with a digitalized business – be it a bank, streaming service or social media platform – due to the bother of switching service providers.

The idea is to give consumers more choice, while levelling the playing field for innovative start-ups and other businesses through access to more data they can use to improve their services and create new offerings.

At the same time, this change could impose significant obligations on the businesses that will have to deal with data portability requests, whether as data transferors, data recipients or both. They will likely need to strengthen their data collection and storage systems, increase their privacy and cybersecurity safeguards, and develop processes and protocols for managing these requests.

The extent of these obligations remains to be seen, however, as detailed regulations to implement the change will only be developed after the enacting legislation is passed.

Chartered Professional Accountants of Canada (CPA Canada) expects that professional accountants will likely play a critical role in helping design, implement, manage and/or certify compliance processes, within their own organizations or those of their clients. We believe it is important for the public interest to ensure that the implementing regulations strike the right balance between enhancing consumer choice and encouraging innovation while minimizing the extra costs and other burdens that could impede the competitiveness of Canadian businesses.

We also believe that as work on the design of these regulations proceeds, the federal government can benefit from lessons learned in other countries that have granted their citizens similar rights.

This briefing reviews the experiences of other jurisdictions and identifies the issues and challenges encountered when implementing data portability. Drawing from this insight, we also highlight how these experiences can help guide the development of a made-in-Canada approach.

In summary, our key observations are as follows:

- Data portability could drive innovation among Canadian businesses and produce economic benefits.
- Canadian businesses would benefit from certainty over the types of data and level of detail that they will need to make portable, based to some extent on the data's potential future usefulness to the individual.
- Verifying that users are who they claim to be addresses a significant privacy and cybersecurity risk for data-controlling companies, as nefarious actors may attempt to utilize data transfer processes to gain access to sensitive personal and corporate data. Sector-specific standards for authentication could improve certainty and ease this burden of user authentication.
- Setting up and maintaining processes for handling data portability requests is one of the biggest business costs. These expenses could be reduced by setting clear standards for the technical format of data transfers.
- Businesses need clarity regarding their legal responsibilities over what happens to the data they transfer to others. Ways should be established for data transferees to show they have adequate data privacy and protections capabilities in place (e.g., codes of conduct, accreditation).
- To reduce the burden on Canadian businesses complying with multiple data portability regimes, Canada's federal regulations should be aligned with rules in place or in the works in the provinces and our country's major trading partners.

Ultimately, as participants in a workshop organized by the Federal Trade Commission (FTC) in the United States pointed out, privacy and cybersecurity risks could jeopardize the benefits of data portability, which highlights the importance of striking the appropriate balance between minimizing those risks, while also maximizing privacy, innovation and competition objectives.[1]

Finally, this report concludes that in this rapidly evolving area, the federal government should consider its approach to data portability regulation by examining lessons learned in other jurisdictions and consulting closely with innovative businesses and other stakeholders.

1 Gabe Maldoff, Jayne Ponder, Kayvan Farchadi and Claire O'Rourke, "Five Key themes from the FTC's Data Portability Workshop," *Inside Privacy*, September 30, 2020.

What is data portability, and why is it important?

In February 2018, the House of Commons Standing Committee on Access to Information, Privacy and Ethics completed a review of PIPEDA and recommended a number of important changes, which included providing Canadians with a right to data portability.

According to the committee's final report, "... individuals must remain as free as possible to use their personal information as they wish. However, this freedom should not be limited to the ability to consent to the collection, use and disclosure of their personal information or to withdraw that consent. The Committee believes that it is just as important for individuals to be able to transfer their personal information between service providers so it can be reused."[2]

> Giving consumers more control over this type of personal information is one reason why the European Union introduced the world's first broad right to data portability in 2016.

There are many types of data that consumers may wish to transfer from one service provider to another. These include not only basic contact and identifying information but also web browser histories and bookmarks, photos with tags and comments, recipes, playlists, banking and financial records, health and wellness data, and data from smart meters and products connected to the Internet of Things.

Giving consumers more control over this type of personal information is one reason why the European Union (EU) introduced the world's first broad right to data portability in 2016:

2 House of Commons, *Towards Privacy By Design: Review Of The Personal Information Protection And Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics, February 2018.

> *The purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.*
>
> *Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers. It will facilitate switching between different service providers, and will therefore foster the development of new services in the context of the digital single market strategy.*[3]

As data pools grow larger and data analytics capabilities encompass combinations of ever more diverse datasets, the value of transferable personal data should continue to increase. For consumers, the benefits will go beyond convenience and ease of switching providers as businesses grow more adept at deriving insights from personal data to improve their products and services, and how they deliver them.

According to the Data Transfer Project,[4] data portability opens possibilities for a wide range of valuable new services for individuals, such as:

- richer information on their health and wellness by combining data from healthcare systems, wearables and other sources
- improved personal finances through access to detailed transaction and other data across accounts and institutions
- better access to public and private services
- greater oversight and transparency over their personal data
- more ability to secure their personal data, including backup or archival of important information and easier recovery from account hijacking[5]

> The productivity and competition benefits enabled by personal data mobility would add £27.8 billion (about $50 billion Canadian) to the U.K.'s gross domestic product.

3 Article 29 Data Protection Working Party, Guidelines on the right to data portability, adopted on December 13, 2016; as revised and adopted on April 5, 2017.

4 The Data Transfer Project is a collaborative open source initiative to develop concepts and tools to facilitate customer-controlled bulk data transfers between two online services. Members include Google, Facebook, Twitter, Apple, and Microsoft.

5 Data Transfer Project, *Data Transfer Project Overview and Fundamentals*, July 20, 2018.

In 2018, a U.K. government-commissioned report concluded that personal data mobility "can be a vital stimulus for the next major stage of digital growth."[6] This report's economic analysis estimated that the productivity and competition benefits enabled by personal data mobility would add £27.8 billion (about $50 billion Canadian) to the U.K.'s gross domestic product, and that the contribution of digital innovation enabled by personal data mobility would likely be even greater.

The report argued that "Personal data mobility can drive fresh growth by creating an environment where empowered individuals can safely make valuable use of their personal data, and consent to its use by others in new data-driven services and technologies. In short, delivering benefit to individuals and organisations alike, with significant economic and societal gains."[7]

Indeed, as we will see later in this report, benefits like these are already being realized in some areas, including through the U.K.'s Open Banking initiative.

6 Ctrl-Shift and Department for Digital, Culture, Media & Sport, *Data Mobility: The personal data portability growth opportunity for the UK economy*, 2018.

7 Ibid.

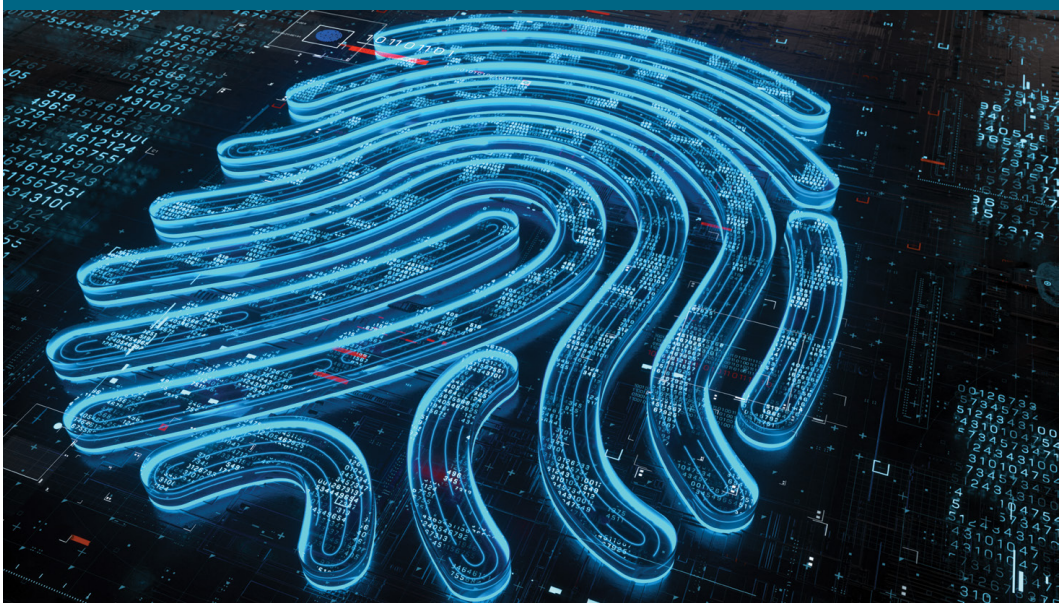
Data portability versus data mobility – what's the difference?

Some people use the terms data portability and data mobility interchangeably. For others, data mobility has much wider scope. The members of the Ctrl-Shift Personal Data Mobility Sandbox, which include Barclays Bank, the BBC, Centrica, Facebook and other organizations, describe the difference as follows:

> *Personal Data Mobility goes beyond Personal Data Portability. Under GDPR [General Data Protection Regulation] people can port personal data from one provider to another, but currently this process tends to be manual and ad hoc.*
>
> *With Personal Data Mobility, personal data flows safely and efficiently to where it can create maximum value. These flows are controlled by the individual ensuring that personal, social and economic benefits are distributed fairly.*[8]

We note that the federal government's Bill C-11 refers to "data mobility," while similar regimes in other countries refer to "data portability," as did the House of Commons Standing Committee on Access to Information, Privacy and Ethics in 2018.

In this briefing, we generally refer to "data portability," except in the context of Bill C-11 and in direct quotes from sources.



8 Ctrl-Shift, *Data Mobility Infrastructure Sandbox: Report June 2019*.

Data portability regimes in other jurisdictions

Approaches in other countries

Many expect that, like numerous other jurisdictions, Canada's approach to data portability will be similar to the right under Article 20 of the EU's General Data Protection Regulation (GDPR), which came into force on May 25, 2018. According to Daniel J. Michaluk, a partner at Borden Ladner Gervais, "Although Canada will not necessarily adopt all the features of the GDPR, it is clearly the model for reform."[9]

The GDPR takes a broad approach to data portability and applies to a wide range of data-processing organizations. While the GDPR does not define data portability specifically, an EU working party defined it as a right that "allows data subjects to receive personal data that were provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without impediments."[10] The data portability provisions of other jurisdictions that are based on the EU model use similar language.

Many expect that, like numerous other jurisdictions, Canada's approach to data portability will be similar to the right under Article 20 of the EU's General Data Protection Regulation (GDPR).

California's Consumer Privacy Act (CCPA), which entered into force on January 1, 2020, is largely similar to the GDPR, although it covers a broader range of private data (e.g., records of website or app interactions).[11] In November 2020, enhancements to the CCPA were passed in the California Privacy Rights Act (CPRA), which will take effect on July 1, 2023. Like the GDPR, the CPRA refers

9 Daniel J. Michaluk, Borden Ladner Gervais LLP, "Canadian privacy law reform is coming – are you ready?" BLG.com, September 18, 2020.

10 Supra note 3.

11 Maria Korolov, "California Consumer Privacy Act (CCPA): What you need to know to be compliant," CSO, July 7, 2020.

to business-to-business transfers of personal information in a structured, commonly used and machine-readable format (although the CPRA only requires the transfer when technically feasible).[12]

Several other states, including Washington and New Jersey, are also considering new privacy legislation. In March 2020, Virginia became the second U.S. state to adopt privacy legislation, including data portability, and Utah is considering a similar bill.[13]

Australia's Consumer Data Right (CDR) took effect in February 2020, allowing consumers to require data holders to share specified categories of data in machine-readable form with accredited service providers.[14] Australia's CDR is being implemented in stages by industry, starting with the banking sector, followed by the energy and telecommunications sectors.

India is taking a different approach to data portability, focused primarily on the banking sector. Unlike the GDPR and similar regimes, India's Data Empowerment and Protection Architecture (DEPA) allows consumer data to be transferred between financial institutions using "just-in-time" digital consent for every data transaction rather than a GDPR-style blanket consent for data transfer and reuse.[15] As described at the FTC data portability workshop, "Under DEPA, users can log into authorized apps and pull together their financial data – such as their transaction histories – that they can then share to obtain loans and other financial services."[16]

Other jurisdictions that have introduced similar legislation on data portability include Singapore, Mexico, Argentina, Brazil and Chile. In the United States, the FTC is seeking to develop a data portability regime that would apply federally, and it has undertaken consultations that look to the GDPR and CCPA as possible models.

12 Wirewheel, "CPRA vs. CCPA vs. GDPR: How the Difference Impacts Your Data Privacy Options," 2020.

13 Cat Zakrzewski, "Virginia governor signs nation's second state consumer privacy bill," The Washington Post, March 2, 2021.

14 Linklaters, "Data Protected – Australia," March 2020.

15 Competition Policy International, Inc., Data To Go: The FTC's Workshop on Data Portability, CPI Antitrust Chronicle, November 2020.

16 Ibid.

Measures in Canadian provinces

A number of Canadian provinces are set to update their privacy laws and bring them more in line with the GDPR:[17]

- In October 2020, Quebec's Bill 64 was passed in principle, granting a new data portability right to consumers in the province among other changes.[18]
- In Ontario, consultations on proposals to improve privacy protection, including a data portability right, closed in October 2020.[19]
- In December 2020, British Columbia established a special committee to review the province's Personal Information Protection Act with a focus on the provisions in Bill C-11. The special committee will also consider input received from public consultations prior to the recent election.[20]
- In January 2021, Alberta's information and privacy commissioner called for updated privacy legislation, including data portability, due to "the sweeping technological change brought about by the COVID-19 pandemic and a movement to change similar legislation in other jurisdictions."[21]

While there is a lot of movement in Canada and internationally, these laws are relatively new or not yet in force, so there is little experience or empirical research to date to gauge their impact on businesses. In the following pages, we explore some of the biggest issues identified in other jurisdictions in some of the available studies, papers and government consultation documents.

The CPPA's interaction with other data privacy regimes

Depending on where they do business, data-controlling companies in Canada may have to comply with multiple data privacy regimes, including different requirements for data portability. These may include Canada's federal and provincial laws, the GDPR, the CCPA in California, and the U.S. federal and state regimes in development.

When the GDPR took effect in the EU in 2018, its higher standards relative to PIPEDA, including the new data portability right, created obstacles for Canadian companies doing business in the EU. Since then, many Canadian companies have aligned their privacy practices with the GDPR and, more recently, the CCPA.

17 In Canada, the CPPA would apply, like PIPEDA it replaces, to federally regulated corporations and to private companies in provinces and territories that do not have their own privacy legislation.

18 Assemblée Nationale du Québec, Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, tabled June 12, 2020.

19 Government of Ontario, "Consultation: strengthening privacy protections in Ontario,", August 13, 2020.

20 Legislative Assembly of British Columbia, Special Committee to Review the Personal Information Protection Act, December 9, 2020.

21 James Swanson, quoted in Anthony Burden, Field LLP, "Alberta's legislation on Privacy and Protection of Personal Information Needs Review: Commissioner," Mondaq, January 7, 2021.

As small business technical advisor Avery Swartz observed, "Because so many Internet-based companies operate globally, it's easier for them to update their terms of use to meet the most stringent requirement in all countries, instead of having different policies for different regions. Many are choosing to follow the GDPR rules everywhere. They will become the de facto standard for privacy terms worldwide, even in countries that don't police it."[22]

In other words, as lawyer James Swanson put it, companies "usually just comply with the highest bar."[23] However, he adds that certainty is important for business. "When you get into patchworks where Alberta has different rules from the federal government or Ontario, it makes it harder for business. If they are more generally the same it just makes it easier to deal with it."[24]

> The more harmonized privacy laws are, the easier it will be for businesses that have to comply with more than one data protection regime.

The more harmonized privacy laws are, the easier it will be for businesses that have to comply with more than one data protection regime. While it is important to develop federal data portability regulations that are appropriate in the Canadian context, aligning these rules with provincial and other national regimes should help support the efficiency and competitiveness of Canadian businesses.

22 Avery Swartz, "Europe's GDPR rules mean big changes for businesses in Canada," The Globe & Mail, May 17, 2018.

23 Supra note 21.

24 Ibid.

Implementing data portability – issues and challenges

"Implementing data portability is a time-consuming, resource-intensive, and highly technical challenge," according to the U.S. Chamber of Commerce's submission to an FTC workshop on the potential benefits and challenges of data portability.[25]

For the years 2017-2019, data-controlling organizations consistently ranked data portability among the top three most difficult GDPR obligations to comply with in annual surveys by the International Association of Privacy Professionals (IAPP).[26] A separate study from the Information Technology and Innovation Foundation (ITIF) pegged the cost of implementing EU and California-style data portability regulations across the U.S. federally at about US$510 million.[27]

There is no question that businesses would face costs to develop and maintain the infrastructure needed to enable data portability and other data subject rights (e.g., access, correction, deletion). How steep those costs will be may depend on a number of factors, many of which could be influenced by the implementing regulations. We explore some of the most important factors below.

Scope of portable data

Developing and maintaining a data management infrastructure to service data portability and other data subject requests is among the most significant compliance costs for businesses.[28] Companies need to set processes to allow them to store, find and update requested personal information, and to then transfer it in appropriate formats to other organizations on request.

As the U.S. Chamber of Commerce observes, "The process of revising and implementing new technical measures and data management protocols becomes more complex and problematic as the breadth and detail of the dataset covered by portability requirements grows."[29]

25 Chamber of Commerce of the United States of America, Comments to the Federal Trade Commission's Data Portability Workshop, August 21, 2020.

26 International Association of Privacy Professionals and EY, *IAPP-EY Annual Governance Reports 2017 – 2019*, available at https://iapp.org/resources/article/iapp-fti-consulting-privacy-governance-report-2020/

27 Alan McQuinn and Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law," Innovation Technology and Innovation Foundation, August 2019.

28 Ibid.

29 Supra note 25.

Generally, current data portability regimes apply to information directly provided by users, such as contact information and preferences, as well as observed data, such as web browser histories. Data that an organization infers using proprietary algorithms, for example, to predict a user's behaviour, are generally out of scope.

Some have argued for additional limits on the extent of data that is subject to portability to reduce the costs of servicing these requests and provide more certainty for businesses on the scope of this obligation.

In a 2019 white paper, Facebook asked whether there are cases where the operational burden on businesses – especially start-ups and smaller providers – outweighs the consumer's interest in exporting their data. "For example, a service's data about a person's use of a service could include a list of every page or piece of content the person has viewed within a certain period, every link he or she has clicked on, and every notification he or she has received… The process of making this log data portable could be challenging, and the benefits to the user might not always be obvious…"[30]

> Having a well-defined set of data categories will reduce compliance costs and provide certainty for individuals and organisations on the data to be ported.

Singapore has handled this issue by applying its data portability regime to sector-specific "white-listed data sets," tailored for each industry and identified by the Personal Data Protection Commission (PDPC), industry stakeholders and other relevant regulators. For example, white-listed data on consumer spending history only include specific types of data on purchases and payments, while white-listed utilities consumption history data include specific data such as mobile data and electricity usage.

According to the PDPC, "Having a well-defined set of data categories will reduce compliance costs and provide certainty for individuals and organisations on the data to be ported under the Data Portability Obligation."[31]

30 Facebook, Charting the Way Forward: Data Portability and Privacy, 2019.

31 Personal Data Protection Commission (Singapore), Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions, January 20, 2020.

Canadian businesses would benefit from certainty over the types of data and level of detail that they need to make portable, based to some extent on the data's potential future usefulness to the individual.

Customer authentication requirements

Issues related to authentication are persistently named as a top concern for data transferring companies, including in the IAPP's 2020 survey of data-controlling organizations.[32] To preserve data privacy and prevent potential cybersecurity breaches, it is critical for businesses to verify that someone requesting a data transfer really is who he/she claims to be. This is even more imperative as nefarious actors may attempt to utilize the data transfer process to launch a cyberattack against a company and, in the process, potentially gain access to sensitive personal and corporate information.

A panelist at the FTC's 2020 data portability workshop[33] observed that customer authentication was a significant obstacle to the use of the U.K.'s Open Banking program by individuals, especially when they had to go through multiple steps to allow their bank to share their data. Similar difficulties were noted in the U.K. health sector for both patients and data-controlling organizations.

Current methods being refined by the private sector involve combinations of reference databases, data matching, and biometric and multifactor identification. However, one workshop panelist noted that in the context of the financial sector, such methods would impose high costs on financial institutions and customers alike, potentially limiting customer access.

Many financial institutions have had "Know Your Customer" (KYC) processes in place to counter financial crime and money laundering for years. If authentication remains a costly challenge for large financial institutions with existing KYC frameworks and significant resources, it seems likely that smaller businesses building authentication processes from scratch would face even more costs and difficulty. As we previously indicated in a submission to the federal government, "smaller entities, such as SMEs [small and medium-sized enterprises], non-governmental organizations (NGOs) and charities, may not all have the necessary digital technology and literacy (including skills) to move data such as personal information to another organization in a safe and efficient matter."[34] This may of course hinder the ability of smaller

32 International Association of Privacy Professionals and FTI Consulting, IAPP-FTI Consulting Privacy Governance Report 2020, December 2020.

33 Supra note 15.

34 CPA Canada, Submission in response to: Strengthening Privacy for the Digital Age, January 2020.

organizations to develop robust authentication processes and cybersecurity safeguards. This can ultimately make them more vulnerable to cyber attackers looking to target and exploit these digital vulnerabilities.

Security concerns also arise over data transfer requests made by one person on another's behalf. Several respondents to Singapore's data privacy consultation questioned how data porting requests would be handled, for example, for joint account holders, supplementary credit card holders, insured parties and estate executors.[35]

In the FTC consultation, it was suggested that as part of a new U.S. data portability regime, the U.S. government may need to set standards to give banks certainty over which authentication procedures are appropriate. Similar sector-specific standards could improve certainty and ease the burden of user authentication in other industries.[36]

Reducing the processing burden on organizations

In the ITIF's estimation of the costs of a federal data portability regime to U.S. businesses, the majority of expected costs – US$340 million of the total US$510 million – relate to the processing of data subject requests. The ITIF notes that these requests will not only be made online but also by phone, mail or in person, and that human processing can increase costs significantly.[37]

> In the ITIF's estimation of the costs of a federal data portability regime to U.S. businesses, the majority of expected costs – US$340 million of the total US$510 million – relate to the processing of data subject requests.

Affected organizations need to set up and maintain the necessary infrastructure to handle data portability and other data subject requests. Experience with the GDPR shows that these processes can be labour-intensive for many businesses. In IAPP's 2020 survey of data-controlling organizations

35 Supra note 31.

36 Supra note 15.

37 Supra note 27.

subject to the GDPR, 62 per cent of respondents reported having teams dedicated to servicing data subject requests, a significant increase from the year before (52 per cent).[38]

Despite having dedicated teams, it took many of these organizations considerable time to service data subject requests. While about 30 per cent responded within two days, just over half took a few days to two weeks, and 12 per cent took a month or longer. About half of respondents used some degree of automation to process requests; the processes of the other half were entirely manual.

Fifteen per cent of the data subject requests received in 2020 by these companies were requests for data portability. A separate 2019 study on the impact of GDPR in practice shows that data portability requests present particular challenges.[39] For this study, researchers made 230 real-world data transfer requests and examined how businesses responded. Only about 75 per cent of the requests were completed successfully. Even among these requests, many of the file formats failed to meet GDPR requirements. The researchers also found some confusion among these businesses about consumer's data rights more generally.

These results align with the European Commission's own findings in its post-implementation review of the GDPR conducted in 2020.[40] The Commission found that many data-controlling organizations struggled with the requirement to provide data in a "structured, commonly used machine-readable format" due to the lack of standards for what such a format entails, which varies considerably by industry. The Commission also found that only organizations in particular sectors, such as banking, telecommunications and utilities, had implemented the interfaces needed to satisfy data portability requests in an appropriate format.

38 Supra note 32.

39 Janis Wong, Tristan Henderson, "The right to data portability in practice: exploring the implications of the technologically neutral GDPR," School of Computer Science, University of St Andrews, May 22, 2019.

40 European Commission, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, June 6, 2020.

The Commission's European Strategy for Data, adopted in February 2020, mandates the development of technical interfaces and machine-readable formats to facilitate data portability. However, even though companies have started offering their data in structured, commonly used and machine-readable formats to comply with the GDPR or similar legislation, it has been observed that in most cases those formats are not compatible with one another.[41]

The researchers of the 2019 practical study similarly concluded that future work was needed to help data controllers comply with the data portability right: "We suggest that various stakeholders work together to decide the most appropriate method for supporting the [right to data portability] whether that may be the development of guidance, standards or codes of conduct. Further empirical research … would provide a more holistic view of the [right] in practice."[42]

In its submission to the FTC, the U.S. Chamber of Commerce also calls for appropriate technical standards as part of a potential U.S. federal data portability regime. "Without standards – which are best developed by standard-setting bodies that are governed by a voluntary and consensus-based approach – businesses and regulators alike have been unable to translate [the EU data portability provision] into meaningful outcomes for consumers."[43]

> Without standards – which are best developed by standard setting bodies that are governed by a voluntary and consensus-based approach – businesses and regulators alike have been unable to translate [the EU data portability provision] into meaningful outcomes for consumers.

41 Data Transfer Project, Why do we need the DTP, July 20, 2018.

42 Supra, note 39.

43 Supra, note 25.

Based on the experience in the EU, it has been warned that similar issues could arise in Canada unless issues involving data interoperability are clarified. According to former Privacy Commissioner of Canada Jennifer Stoddart and Fasken lawyer Julie Uzan-Naulin, "Exercising this right to data portability turned out to be fairly difficult in the EU. It will likely be even more so in Quebec and Canada due to the lack of detailed technical guidelines from the data protection authorities or the lack of shared standards or technological codes among businesses."[44]

A report commissioned by the U.K. government expressed a similar view in 2018: "The development of common and robust standards, technologies and services is vital to the creation of a healthy market that has personal data mobility at its core. Until these are developed, the risks and costs of data mobility for all of the stakeholders are significantly increased, and the rate of market development and access to the opportunities is significantly slowed."[45]

Application protocol interfaces and interoperable platforms

The U.K.'s Open Banking project, which relies on common standards for application protocol interfaces (APIs), data formats and security, highlights the importance of secured APIs and open-source technologies in realizing data portability's promise in practice. This project was launched after an investigation by the U.K. Competition and Markets Authority (CMA) found that the country's oldest and largest retail banks were taking advantage of the fact that consumers rarely move their accounts even when fees are high.

As described in a presentation to the FTC, "The CMA required the UK's nine largest banks to develop APIs … that would allow bank customers to securely share their financial data with regulated third parties so a broad range of businesses could compete to provide financial services. Two years after implementation, there are over a million active users of UK Open Banking and over 700 providers of UK Open Banking services, with no material security events."[46]

44 Julie Uzan-Naulin and Jennifer Stoddart, Fasken LLP, "Right To Data Portability: True Data Portability Or Simply An Updated Version Of The Right Of Access?", September 14, 2020.

45 Supra note 6

46 Supra note 15.

Now in its third year, the number of consumers using Open Banking is closer to 3 million. According to a representative from the Open Bank implementation authority, "... [I]ndividual consumers and small businesses are already seeing the benefits of the ecosystem and functionality we have put in place. This work serves as a natural blueprint for how the 'open' philosophy can be extended to everything from open finance to open telecommunications, thereby giving customers greater control and greater benefits."[47]

The use of APIs and interoperable platforms increases data portability's usefulness since they enable the transfer of usable, real-time data, rather than static, moment-in-time information that transferee businesses may be unable to reuse. In the absence of APIs, data transfers are sometimes performed through the "screen scraping" techniques, which require individuals to share their login credentials with third parties to enable them to access and collect their data from different platforms (mostly online banking ones). As the Standing Senate Committee on Banking, Trade and Commerce heard from witnesses during its study on open banking in 2019, screen scraping increases the risks of identity theft and fraud as well as cybersecurity risks.[48] In this regard, professor Teresa Scassa from the University of Ottawa observes that: "A regulated framework for data mobility is seen as much more secure [than screen scraping], since safeguards can be built into the system, and participants can be vetted to ensure they meet security and privacy standards."[49]

The use of APIs and interoperable platforms increases data portability's usefulness since they enable the transfer of usable, real-time data.

47 Open Banking, "Three years since PSD2 marked the start of Open Banking, the UK has built a world-leading ecosystem," January 13, 2021.

48 Standing Senate Committee on Banking, Trade and Commerce, Open Banking: What it Means for You, June 2019.

49 Teresa Scassa, "Data Mobility (Portability) in Canada's Bill C-11," January 12, 2021.

Collaborative projects such as the Data Transfer Project are underway to develop common APIs, interoperable platforms and other necessary infrastructure. The project's goal is to develop an open-source, service-to-service data portability platform that makes the transfer of data technically feasible across potentially all organizations. In the U.K., the Control-Shift Data Mobility Sandbox project brings together business, governments, consumer groups and consumers to design and test the infrastructure and tools needed to make data portability easier and more controllable for consumers.

Verifying the suitability of data transferees

In addition to the challenges of ensuring data is provided in formats that recipients can use, there are questions over the extent of the transferor's responsibility for the personal data they transfer. For example, panelists at an FTC workshop questioned whether data transferors would face risks and responsibilities if they were to transfer data to a service provider with inadequate privacy or cybersecurity protections. Questions and concerns around whether they would they be liable for any onward transfers or other downstream uses of the transferred data were also raised.[50]

In response to Singapore's data portability consultations, some pointed to the need for clear limits of liability for transferring organizations in discharging their obligations and sought clarity on the liability for data breaches arising from the porting of data, as well as the accuracy of data transferred to another organization. Singapore's PDPC indicated that data recipients would have the same obligations as they would with any other personal data in their possession in terms of protecting it, ensuring its accuracy, and only using it for purposes that have been notified.

The PDPC is also prescribing binding, sector-specific codes of conduct for consumer safeguards, counterparty assurance, interoperability and data security that require entities to have certain protections in place before they receive user-requested data. As noted earlier, these codes only apply to "white-listed data sets" identified by the PDPC jointly with industry stakeholders and sectoral regulators.

50 Supra note 15.

> Another alternative is to introduce a form of accreditation for recipient organizations so they can demonstrate their data protection and security capabilities to consumers and transferring businesses.

Another alternative is to introduce a form of accreditation for recipient organizations so they can demonstrate their data protection and security capabilities to consumers and transferring businesses. Australia recently proposed changes to its CDR that would create pathways for service providers to become "accredited data recipients," with various tiers of accreditation to help foster start-ups and smaller providers. The proposals also put the Australian Competition & Consumer Commission in charge of accrediting potential data recipients, establishing and maintaining a Register of Accredited Persons, and monitoring and enforcing compliance.

Despite Australia's special provisions made for start-ups and smaller businesses, many of them may not have the financial resources, skills, time or knowledge needed to seek accreditation. Not only does this create a burden for these businesses, it could also create barriers to entry for new, smaller players and discourage the type of competition that data portability is expected to enable.

Conclusion

In this report, we highlight some of the considerable costs and risks that a new data portability regime could entail for Canadian businesses. However, if implemented with a set of well-designed regulations, data portability could drive innovation among Canadian businesses and produce economic benefits.

As Facebook's white paper observes:

> *To build portability tools people can trust and use effectively, we should develop clear rules about what kinds of data should be portable and who is responsible for protecting that data as it moves to different providers.*
>
> *Without an enabling infrastructure, data portability opens up new risks for consumers, organizations and governments alike. Only working together can these stakeholders create a market that will enable us to realize the benefits.*[51]

The U.K. government-commissioned report emphasized the importance of ensuring that data-related regulation is up-to-date and structured in ways that support growth. "The fast-moving and emergent nature of the personal data market means that a traditional approach to regulation will create blockers and limit the market's potential."[52]

The report recommended developing a regulatory structure through close consultation and collaboration among government, innovators and regulators, followed by regular review of these regulations to support the progress of data portability.

In developing its approach toward data portability regulation in Canada, we believe the federal government would do well to consider the experiences of other jurisdictions discussed in this report. With the rapid and ongoing digitalization of our economy, it will be important for the government to engage with organizations and business groups to help ensure Canadian individuals can safely and securely enjoy the consumer benefits that data portability brings, while mitigating the burden and enabling the potential opportunities for Canadian businesses.

51 Supra note 30.

52 Supra note 6.

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
CPACANADA.CA