Business Council of Canada

Dgen

Data-Driven: Canada's Economic Opportunity

Issues Paper

Prepared by Dgen for the Business Council of Canada

July 22, 2019 (Updated August 22)

Table of Contents

Executive Summary

1. Introduction

Data is transforming our economy and society. Advances in digital technology allow us to gather and store ever-more data, enabling smarter and faster decisions that grow the economy and improve our lives. But they are also giving rise to new public policy questions. How do we get the right data to the right place at the right time? How do we distribute the benefits? And how do we protect people's privacy, security, and rights?

Countries are launching national strategies to realize the opportunities and address the challenges of a data-driven world. Canada can be a leader in this world, but we need to move fast. In May, the federal government announced a new *Digital Charter* – a set of cross-cutting principles that will guide reforms to federal privacy and competition laws, as well as other frameworks impacting data. The stakes are high, and Canada cannot afford to get it wrong.

This paper is the first step of a research initiative launched by the Business Council of Canada to develop concrete recommendations on what Canada's reforms should entail. Prepared by Dgen, a consultancy, the paper takes stock of key trends, issues, and questions on the minds of policymakers. Rather than draw conclusions, the goal of the paper is to drive discussion with Canadian industry to identify priorities and policy options that the study will address in subsequent work.

2. A Data-Driven World

The proliferation of high-speed telecommunications, sensors, and digital devices is producing unprecedented volumes of consumer and industrial data every day. Organizations are using AI and advanced data processing to transform this data into economic and social value – from improved health, transportation, and government services, to more efficient energy use and farming practices. According to McKinsey, AI could add around 16 per cent to global economic output by 2030, while AI-related innovation in products and services could add another seven per cent.

However, these benefits do not happen accidently. Organizations need to invest in collecting, sharing, and processing data. Statistics Canada estimates that Canada invested up to $40 billion in data last year alone – with nearly 80 per cent coming from the private sector. The challenge for governments is to maximize the economic potential of data, while protecting the rights and security of their citizens. No country has found all the solutions. We can develop a 'made-in-Canada' model that strikes the right balance between market forces and regulation, that aligns with the provinces and our trading partners, and that businesses can operationalize.

3. Policy Issues

Canadian policymakers are wrestling with several key issues and dilemmas related to the rising importance of data in the economy and society. We can look at how other

countries address these issues and consider what is appropriate for our circumstances. This section lays out the key questions policymakers want industry to help answer.

3.1 Privacy and security:

Individuals and businesses need confidence that organizations are protecting their privacy and confidential data. Organizations should have effective measures to protect data from a range of harms, including accidental release, fraud and theft, unauthorized access, and inappropriate use.

- Consent and transparency: How can companies help customers and employees better understand how their data is being used? How do we ensure that consent is meaningful? What alternatives to consent-based privacy should Canada consider? What uses of personal data should we prohibit?

- Algorithms and automated decision-making: Should companies disclose how algorithms and automated decisions impact individuals? Are there other ways to protect people from biased or inaccurate models? Should policy address the use of algorithms in industrial applications too?

- Right to erasure: Under what conditions can individuals require organizations to delete their personal information? What data can organizations retain? How can organizations erase this data without affecting the quality of their datasets or algorithms?

- Enforcement: How can we strengthen compliance with Canada's privacy laws? Is there a role for increased enforcement powers and penalties? Who should administer these? How can we prevent stronger enforcement from deterring business investment in data-driven innovation?

- Cybersecurity: What can the government do to help businesses combat cyberattacks? Should government require business to adopt certain cybersecurity practices? How can we promote the growth of the cybersecurity insurance market?

3.2 Ownership and control

Markets work best when there are clear property rights. While determining who 'owns' data is problematic, Canada could better define the different types of data and clarify the respective rights and interests of businesses and individuals.

- Consumer data rights: To what extent should consumers be able to move personal data between different service providers? What is the best approach to facilitate data portability? Is regulation needed? If so, should it be sector-by-sector or economy-wide?

- Business data rights: Where should the line be drawn between personal and business data? Do businesses need more tools to assert and protect their rights to commercial or industrial data? Are contractual mechanisms enough?

3.3 Competition

Data gives companies a competitive advantage, creating a healthy incentive to invest in it. But data can also be a source of market power, reducing competition when it is concentrated in the hands of a few firms.

- Competition policy: Is data concentration hurting competition in Canada? In which sectors is this a concern? Does the Competition Bureau have the mandate and tools it needs to do its job?

- Foreign investment policy: What is the impact of foreign acquisitions of data and AI companies on competition and innovation in Canada?

3.4 Public sector data

How governments collect, manage and share data has economic implications. Canada may need to revisit the terms of access to, and use of, personal and confidential business data. There are also opportunities for government to leverage its own data assets to provide better public services or fuel private sector innovation.

- Government access to data: What types of data are in the public interest? Under what terms should the government be able to compel or access private or confidential data? What process should government follow?

- Sharing public sector data: Is Canada doing enough to release valuable public data sets? How should government prioritize data for release? What are the barriers? On what terms should private companies be able to access public data? Who should cover the costs?

3.5 Cross-border data flows

As the implications of data for public policy grow, governments are asserting more control over the data in their jurisdiction. This is leading to local storage requirements and restrictions on cross-border data flows. Moreover, companies must comply with a growing patchwork of different rules, both internationally and within Canada.

- Data localization and rules on cross-border flows: How are local storage requirements impacting data-driven innovation in Canada? Are there cases in which data localization is necessary for the public interest? What requirements should businesses meet when storing and processing sensitive data abroad?

- Regulatory coordination: To what extent should Canada align its privacy laws to those of other jurisdictions, such as the European Union? How can we better

align data rules between the federal and provincial governments? In which sectors is alignment needed the most?

- International agreements and norms: How should free trade agreements address cross-border data flows? Which forums should Canada use to influence global norms around data and AI governance?

3.6 Data Infrastructure

Canada may need new industry standards and institutions to support a data-driven economy. Important issues include the conditions of access to this infrastructure, as well as how it will be governed and financed.

- Industry standards, codes of conduct, and certification: Does Canadian industry need more common APIs and data governance standards? If so, in what areas? Should the government formally recognize codes, standards, or certifications?

- Data libraries and trusts: Which sectors of the economy would benefit from pooling their data? What role should government play in this? Are 'data trusts' a solution to manage access to, and use of, sensitive data? How should trusts be governed and who should pay for them?

1. Introduction

Data is transforming our economy and society. Advances in digital technology allow us to gather and store ever-more data, enabling smarter and faster decisions that can grow the economy and improve our lives. But they are also giving rise to new public policy questions. How do we get the right data to the right place at the right time? How do we distribute the benefits? And how do we protect people's privacy, security, and rights?

Countries are launching national strategies to realize the opportunities and address the challenges of a data-driven world. Canada can be a leader in this world, but we need to move fast. In May 2019, the federal government announced a new *Digital Charter* – a set of cross-cutting principles that will guide reforms to key policy frameworks impacting data, from privacy and competition law to industry and government standards. Yet there is no clear consensus around what, exactly, these reforms will entail.

Given what is at stake, the Business Council of Canada launched a research initiative to develop concrete policy recommendations in these areas. This paper is the first step in that initiative. Prepared by Dgen, a consultancy, the paper takes stock of key trends, issues, and questions on the minds of Canadian policymakers. Rather than draw conclusions, the goal of the paper is to drive discussion with Canadian industry to identify priorities and policy options that the study will address in subsequent work.

The first half of the paper reviews the economic, business, and political dimensions of an increasingly data-driven world. The second half outlines key policy issues and questions in the following areas: privacy and security, ownership and control, competition, public sector data, cross-border data flows, and data infrastructure.

2. A Data-Driven World

Advances in digital technology allow organizations to gather more data than ever before, and to use that data to make smarter and faster decisions, creating value across every sector — from improved health, transportation, and government services, to more efficient energy use and farming practices. This section reviews the rise of data as an economic asset, a driver of business competitiveness, and an increasingly controversial subject of public policy. It shows the need for Canada to have a national strategy that both protects and unlocks the value of data for businesses, consumers, and citizens.

2.1 The Economics of Data

Data is an essential part of today's economy. It makes up a growing share of global GDP, international trade, and business investment. However, as an 'intangible' asset, data has unique characteristics that require new ways of thinking about economic policy.

Data is not new. For thousands of years, humans have been recording observations as symbols, numbers, and letters. What is new, however, is the volume of data that is being produced each day as a result of the proliferation of devices, services, and sensors. Increased connectivity allows us to copy, move, store, and process data cheaply, without degradation, at rapid speeds around the globe. Every day, 3.7 billion people send 500 million tweets, 65 billion WhatsApp messages, and 294 billion emails. And that's just communication by live individuals.[1] The growth of the Internet of Things (IoT), which will dramatically increase the number of connected devices, and the advent of faster 5G telecommunications networks, will only accelerate this trend of 'datafication' throughout all aspects of industry and society.

The value of data does not come from its increased supply; it comes from what we can do with it. Advances in cloud computing, processing power, AI, and data science enable us to turn raw data into new insights, resulting in better and faster decisions that can solve problems and ultimately improve our lives. That could mean a commuter shaving valuable time off the drive to work, a farmer planting seeds in locations that will yield a larger harvest, or a healthcare worker getting mental health services to those who need them most urgently. McKinsey estimates that AI alone could add 16 per cent to global economic output by 2030, with AI-related innovation to other products and services adding another seven per cent.[2] It is this economic potential that is driving the demand for data and turning it into such a highly prized resource.

We are only beginning to understand how big the data economy is. McKinsey, for instance, estimates that cross-border data flows currently contribute more to global GDP than trade in goods.[3] In fact, they argue that the slowdown in international trade and investment since the 2008 financial crisis may not be a reversal of globalization, as some have suggested, but rather a sign of how data flows are starting to substitute for traditional flows of goods, services, and capital.

In Canada, investment in data has grown rapidly in recent years. New research from Statistics Canada estimates that organizations invested up to $40 billion in data, databases, and data science last year – greater than the amounts spent on industrial machinery, transportation equipment, intellectual property, or research and development.[4] Already, the stock of Canada's data assets could be as high as $217 billion, comparable to Canada's bitumen reserves, which were valued at $300 billion in 2017.

The rise of data is part of the broader rise of an 'intangibles economy', which operates in fundamentally different ways than the traditional economy.[5] Intangible assets, such as data and IP, are unlike tangible investments in machinery or buildings. First, they can be scaled at no cost. Data can be copied and used by many people at the same time.

Second, intangibles have strong synergies. The value of data increases when it is combined with other data, algorithms, or software. Third, intangibles often have significant spillovers. There is nothing, for instance, to prevent companies from scraping the same data from the Internet or taking the same detailed satellite photos. Finally, investments in intangibles are often sunk costs. Companies often collect data for a distinct purpose or format and its value can depreciate fast, making it hard to resell.

These unique properties make investments in data and other intangibles less certain and more likely to be contested by others. As a result, companies on average will underinvest in these assets. But it also means that those who do invest can quickly become dominant. In "winner-take-all" markets, companies with initial advantages have the incentive to invest further in their position, while those who are behind do not – leading to a growing gulf between the best and the rest. This may especially be the case for data and AI. The more data a firm has, the better their predictions will be. Better predictions can help a firm grow, giving them more data to feed into their models.[6]

These dynamics require new thinking about economic policy. The tangible economy has a long history of institutions and norms – property rights, market pricing, standards, and regulations. These enable the efficient exchange of value across individuals and firms. In contrast, the economic model for data is much less developed, which could make it prone to market failures.

2.2 The Business of Data

The private sector is at the centre of the data-driven economy. Industry was responsible for nearly 80 per cent of the data investment in Canada in 2018. [7] Companies decide which problems to solve with data, how to gather the data, and how to extract the right insights. At the same time, data is transforming corporate strategy and business models, as well as relationships with competitors, suppliers, and customers. Any national data strategy must consider the fast-changing operational realities they face.

Companies create data by digitizing processes. Digitizing customer interactions provides a wealth of data for marketing, sales, and product development. Digitizing internal processes generates data that can be used to optimize operations and improve productivity. Data can improve customer intelligence, predict equipment failure, manage product quality and risk, optimize supply chains, and prevent fraud. The applications are effectively endless.

Consumer-facing businesses were early to digitize and leverage data and analytics. But upstream businesses are catching up fast. They are deploying IoT sensors to capture data directly from the physical environment, including production lines, energy generation and transmission, transportation and telecommunications infrastructure, and vehicles used for moving freight and passengers. The ability to transmit this data in real-time through 5G will only further facilitate and accelerate these processes. In fact, McKinsey estimates that by 2025, business-to-business (B2B) solutions will account for 70 per cent of the value created by IoT.[8]

To date, most companies have only realized modest gains from their investments in big data, advanced analytics, and AI.[9] Companies need to clean and integrate fragmented data from multiple sources, break down silos between units and functions, and set internal data-governance standards. Many companies remain preoccupied with classic large-scale IT-infrastructure programs, rather than focused on data management and the capabilities to extract value from them. Data-driven innovation can only happen when it is fully embedded in a company's culture and operations.

In the short term, data helps companies do their current business better. But in the long term, it can transform strategy and entire business models. If Amazon, for instance, becomes good enough at predicting buying habits, they could deliver products before customers order them, leaving them only to pick up the returns when they get it wrong.[10] This would cause a radical shift in how retailers manage inventory, logistics, and warehousing.

Industrial firms are adopting new data-driven strategies too. John Deere's cloud-based IoT platform, for example, collects data from farm equipment and farmers to generate valuable insights on everything from fuel and maintenance needs, to ideal planting times and fertilizer use. These insights attract more farmers to the platform, generating more data. John Deere has gone from selling tractors to selling solutions. Similar examples are emerging in construction, mining, and advanced manufacturing. Data has become a competitive battleground for everyone, where scale matters and companies worry about their competitors getting an upper hand.

In this race, businesses are finding new ways to encourage clients and others to share data. Instead of collecting data as a by-product of other activities, companies are increasingly offering an explicit exchange of value for data. For consumers, that could mean enhanced products or services, or even monetary value, as in the case of loyalty programs. In the B2B market, IT vendors may offer incentives for enterprises to move their commercial or industrial data to a new platform. Equipment suppliers may offer discounts in exchange for the right to access data about the performance of their products. Many companies are differentiating themselves based on their commitment to privacy and data protection. Apple's new advertising campaign, which emphasizes user privacy, is a clear example of this.

2.3 The Politics of Data

Governments play an important role in the data-driven economy. They need to create conditions that will unlock the value of public and private sector data, while protecting citizens from potential harms. Canada has an opportunity to learn from other countries and to build a model that helps businesses compete, gives consumers protection and choice, and makes Canada a global leader in data-driven innovation.

The ubiquitous impact of data is forcing a rethink of public policy in many areas. On the economic front, governments need to establish marketplace rules and norms that will drive competition and encourage investment in data-driven innovation. But the social

and political dimensions of data are equally important. There are concerns about how the use of personal data is impacting individuals, whether through growing surveillance and monitoring, AI bias in employment decisions, or the use of micro-targeting to manipulate behaviour or radicalize voters. There are national security and geopolitical concerns too. Military and intelligence capabilities increasingly depend on data and AI, while the growing reliance on data to manage critical infrastructure is creating new cyber vulnerabilities.

Many countries have launched cross-cutting national data strategies. They hope that comprehensive approaches will ensure alignment across government agencies and business to leverage the potential of data, while addressing the economic and non-economic challenges. Singapore's 'Smart Nation' strategy, launched in 2014, aims to broadly transform urban life through collaboration with businesses and citizens, impacting sectors across the economy, from transport to health. In 2016, Australia commissioned a major independent inquiry into how to improve the availability and use of private and public sector data, leading to significant legislative reforms affecting how consumers, business, and government access and share data. In 2018, the United Kingdom (UK) announced it would develop a National Data Strategy, building on the country's pioneering work in the area of open data.

Experts have been calling for Canada to do the same. The Centre for International Governance Innovation, for instance, has argued for a national data strategy that would detail an open architecture for technology, standards and rules for data collection and exchange, a framework for privacy, infrastructure for libraries of industry data, cybersecurity protection, a strategy for data-related intellectual property (IP), and a whole-of-government approach to public sector data.[11]

In May 2019, the federal government unveiled its *Digital Charter*.[12] The Charter outlines a set of high-level principles with which to modernize Canada's data frameworks (see Box 1). Canadian business is well-placed to help policymakers think through and operationalize the principles, starting with the associated reviews of federal privacy and competition law, as well as government and industry data practices.

As the federal government modernizes these frameworks, it needs to strike the right balance among regulation, market forces, and competition policy. It will need to consider the division of powers across federal departments and with the provinces, and the interplay with international policy developments. Canada's integration with global supply chains makes interoperability essential. We need a pan-Canadian approach that is compatible with our trading partners, and that our businesses can operationalize.

Box 1: Canada's Digital Charter

1. Universal Access: All Canadians will have equal opportunity to participate in the digital world and the necessary tools to do so, including access, connectivity, literacy and skills.

2. Safety and Security: Canadians will be able to rely on the integrity, authenticity and security of the services they use and should feel safe online.

3. Control and Consent: Canadians will have control over what data they are sharing, who is using their personal data and for what purposes, and know that their privacy is protected.

4. Transparency, Portability and Interoperability: Canadians will have clear and manageable access to their personal data and should be free to share or transfer it without undue burden.

5. Open and Modern Digital Government: Canadians will be able to access modern digital services from the Government of Canada, which are secure and simple to use.

6. A Level Playing Field: The Government of Canada will ensure fair competition in the online marketplace to facilitate the growth of Canadian businesses and affirm Canada's leadership on digital and data innovation, while protecting Canadian consumers from market abuses.

7. Data and Digital for Good: The Government of Canada will ensure the ethical use of data to create value, promote openness and improve the lives of people — at home and around the world.

8. Strong Democracy: The Government of Canada will defend freedom of expression and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institutions.

9. Free from Hate and Violent Extremism: Canadians can expect that digital platforms will not foster or disseminate hate, violent extremism or criminal content.

10. Strong Enforcement and Real Accountability: There will be clear, meaningful penalties for violations of the laws and regulations that support these principles.

3. Policy Issues

> *"Privacy is for us just one facet of the diamond called data. Polishing only that one facet will not reveal the true value of this, the 21st century's great new renewable resource."*[13]
>
> - Peter Harris, Chair, Australia Productivity Commission, and Author, *Data Availability and Use Inquiry*.

Policymakers in Canada are wrestling with several key issues related to data. While attention is often on privacy and cybersecurity, questions about ownership and control of data, data's impact on competition, governance of public sector data, cross-border data flows, and data infrastructure are equally important.

These issues are complex and cross the mandates of different departments and levels of government. And not all them should be resolved through government regulation or intervention. Market competition and industry-led initiatives have an important role to play. Canada should carefully examine the experiences of other countries and consider

what is appropriate for our circumstances. This section lays out the issues and key questions policymakers want industry to help answer.

3.1 Privacy and Security

Individuals and businesses need to have confidence and trust that organizations are protecting their data. Organizations should have effective measures in place to protect data from a range of harms, including accidental release, fraud and theft, unauthorized access, and inappropriate use.

Data privacy and security have become hot button issues in the wake of high-profile data breaches, cyber-attacks, and misuses of data. In 2017, a ransomware attack on pharmaceutical giant Merck put sensitive commercial data at risk, causing $135 million (USD) in damages. The following year, Equifax announced a data breach affecting the personal information of 143 million people. News also came out that third-party apps used Facebook to collect personal information and influence voters in the United States (U.S.) election and Brexit referendum.

There is a risk that a few bad actors or incidents could undermine public trust, even in organizations that are handling data properly. A recent public opinion survey undertaken for Canada's Office of the Privacy Commissioner (OPC) found that 92 per cent of Canadians have concerns about their privacy.[14] A similar share identified cybercrime as a bigger threat to safety and national security than terrorism, corruption, or other criminal activity.[15]

In response to these concerns, governments are strengthening privacy laws that govern how businesses must handle personal data and information. In 2018, the European Union (EU) implemented the *General Data Privacy Regulation* (GDPR). California has also passed the *Consumer Privacy Act*. The U.S. is also exploring its first federal privacy law.

Many policymakers, academics, and commentators have suggested that Canada modernize its private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[16] As part of the *Digital Charter*, the federal government released a White Paper with proposals for updating PIPEDA in several areas.[17] Some of these proposals are explored below and compared to international developments.

Consent and transparency

Consent is a core tenet of PIPEDA, GDPR, and other privacy legislation, giving businesses legal grounds to access and process personal data. This places some responsibility on individuals to self-manage their privacy. Complex, lengthy, or frequently updated privacy policies, however, can make it difficult for individuals to give informed and meaningful consent. The privacy policies of typical websites, apps, and social media sites are 4,000 to 5,000 words, taking approximately 20 minutes to read.[18]

Another problem is that individuals may be unable to give consent when data is 'observed', rather than willingly provided or volunteered. Observed data might include, for example, the online tracking of individuals through website cookies, or through publicly available information, such as court documents or social media postings. Sensors in 'smart cities' or other connected devices can collect personal information inadvertently, especially as technologies like facial recognition become the norm.

To improve on the consent model, the PIPEDA White Paper proposes that organizations provide specific, standardized, plain-language information on the intended use of personal information and with whom it will be shared. While not required, companies could add information on the benefits customers will receive in exchange for sharing their data. Eliminating 'consent fatigue' would create more informed consumers and significantly improve the user experience.

The PIPEDA White Paper also proposes alternatives, or exceptions, to consent when it is not feasible or appropriate. GDPR, for instance, allows organizations to use 'legitimate business interests' as grounds to process data without individual consent. This could be in order to prevent fraud, report possible criminal acts, or manage network security. Canada could explore a similar range of exceptions.

Without explicit consent, however, the onus to protect privacy falls more heavily on the organization handling the data. Organizations would need to more actively consider ethical questions about how they use data, how it affects an individual's interests, and what they can do to mitigate any risks or harms.

Companies may have to institute new practices. 'Privacy by design' approaches, for instance, incorporate privacy into front-end product development. For a mobile app, that could mean not requesting permissions to access user contacts, not requiring social media registration, de-identifying users, or automatically deleting the data of users who have closed their accounts. Certain types of data use could also simply be prohibited. For instance, many countries, including Canada, have barred insurance companies from asking clients for genetic testing data.

Key questions:

- How can companies help customers and employees better understand how their data is being used? How do we ensure that consent is meaningful?
- What alternatives to consent-based privacy should Canada consider?
- What uses of personal data should we prohibit?

Algorithms and automated decisions

While algorithms and automated decisions carry the promise of new efficiencies, services and products, they also have the potential to negatively impact individuals through inaccuracies, bias, or discrimination. A well-known example is how Amazon's hiring model supposedly 'taught' itself that male candidates were preferable.[19] This was

based on using patterns of resume submissions from the preceding 10 years, most of which came from men.

One option is for companies to be more transparent about how data is used in decision-making. GDPR, for instance, requires that businesses be able to show that the correlations applied in an algorithm are meaningful and unbiased. Canada's PIPEDA White Paper proposes companies disclose the use of, and factors involved in, automated decision-making, where the decision is impactful, and why that decision was made. The government has already issued its own directive to federal departments requiring that automated decisions systems generate consistent and interpretable results.[20] This applies to federal contracts with service providers as well.

There are some problems with this approach. In order to explain the decision, the decision's rules must be available. Companies would have to use 'white-box' models that clearly outline the reasons, for instance, that a credit card company decided not to lend to a customer. It could prevent the use of 'black-box' models, which may produce more accurate decisions, yet be harder to explain. Depending on the level of disclosure required, companies might be worried about exposing proprietary information that could put their IP at risk.

Key questions:

- Should companies disclose how algorithms and automated decisions impact individuals?
- Are there other ways to protect people from biased or inaccurate models?
- Should policy address the use of algorithms in industrial applications too?

Right to erasure

In its broadest sense, the right to data erasure, or the 'right to be forgotten,' means individuals can require that organizations delete their personal data. The issue came to prominence in 2014 when an EU court asked Google to remove links to out-of-date information about a Spanish man's bankruptcy history. The right could also be used by an individual who does not want an organization to have certain personal information that could be used to their detriment in, for example, a life insurance or credit application. Both GDPR and California's new privacy law have provisions for the right to be forgotten.

Canada's laws currently require that organizations delete personal information when it is no longer needed. However, the PIPEDA White Paper notes that compliance with this rule may be low. It therefore proposes more specific rights for individuals to request that their data be deleted, defined limits on retention periods, and an obligation for organizations to maintain the integrity of the data by tracking changes or deletions.

The White Paper stops short of proposing a right to remove personal information from search engine listings, a question that is currently before the courts.[21] Canadian journalists are concerned that such a right could lead to a complex and unchecked

system of private censorship undermining freedom of expression and of the press.[22] To address similar concerns, the EU provided exemptions in GDPR for journalistic purposes and academic, artistic, or literary expression.

Key questions:

- Under what conditions can individuals require organizations to delete their personal information? What data can organizations retain?
- How can organizations erase this data without affecting the quality of their datasets or algorithms?

Enforcement

There are calls for stronger enforcement of federal privacy law in Canada.[23] Currently, PIPEDA is administered by the OPC, which acts as an ombudsman, mediating complaints as a neutral third party. Following an investigation, the Commissioner can issue a report with recommendations, enter into a voluntary compliance agreement with an organization, or take the matter to the Federal Court, which can impose fines for certain violations.

In contrast, GDPR gives EU national data authorities stronger powers. They can issue reprimands, order companies to erase or cease processing data, and impose material administrative fines. In the case of the most serious violations, authorities can levy fines worth four per cent of worldwide revenue or €20 million, whichever is greater. European data authorities have started to use these powers. The UK Information Commissioner's Office, for instance, recently announced a fine on Marriott of £99.2 million for the 2018 data breach that exposed personal information of 339 million Starwood guests.[24] It also intends to fine British Airways £183.39 million for a 2018 cyber incident.[25]

While the PIPEDA White Paper stops short of recommending GDPR-style enforcement, it suggests that the ombudsman model may be outdated. The paper proposes giving the Commissioner greater discretion and flexibility to investigate and audit organizations, and to order them to cease certain activities. The paper also suggests enabling Commissioner to refer a wider range of offences to the Attorney General for investigation, with potentially greater fines. As well, it recommends changing the law to give the courts the power to levy statutory damages in certain cases.

The impact of a stronger enforcement mandate needs to be carefully considered. First, it must not conflict with the OPC's other functions. These include research, guidance and education to organizations, and development of codes of practice – all of which require an open and collaborative relationship with industry. Second, with higher penalties, there may be a need for more clarity around what constitutes non-compliance. To that end, the government's White Paper has suggested making the law more precise through a series of 'housekeeping' updates.

Key questions:

- How can we strengthen compliance with Canada's privacy laws?
- Is there a role for more enforcement powers and penalties? Who should administer these?
- How can we prevent stronger enforcement from deterring business investment in data-driven innovation?

Cybersecurity

In addition to tighter privacy rules, regulators are looking at ways to ensure companies have appropriate cybersecurity policies. Although mandatory reporting requirements for breaches of personal information were introduced for businesses in 2018, Canada's approach to cybersecurity tends to favour collaboration over regulation.

That is the basis of Canada's National Cyber Security Strategy, announced in June 2018.[26] The strategy focuses on combatting and defending against cybercrimes by improving information-sharing and collaboration between the public and private sector. The federal government consolidated cyber operations into the new Canadian Centre for Cyber Security, creating one national authority and a single window for the private sector.

However, the federal government may be considering firmer rules. That could include requiring companies involved in critical infrastructure to put in place appropriate cybersecurity policies, perhaps combined with special access to cyber support services from security agencies. A recent report from the House of Commons Standing Committee on Public Safety and National Security goes further and asks the government to "undertake efforts to ensure the digital products and services… are 'secure by design'" and to support vulnerability disclosure programs.[27]

In the U.S., the federal government has considered policy measures to support the still-nascent cybersecurity insurance market.[28] Cyber insurance underwriters would, presumably, demand that companies meet certain cybersecurity standards to qualify for coverage, creating a form of 'soft' regulation.

Key questions:

- What can the government do to help business combat cyberattacks?
- Should Canada require that businesses adopt certain cybersecurity practices?
- How can we support the growth of the cybersecurity insurance market?

3.2 Ownership and Control

Markets work best when there are clear property rights. Determining who 'owns' data may not be possible, but various rights and interests in data clearly exist, largely through a mix of privacy, IP, and contract law. There may be a need to better define the different

types of data, and the associated rights that individuals and businesses can exercise, especially on the matter of 'data portability'.

Consumer data rights and portability

Privacy laws not only protect personal data, they give individuals a level of control and right of access to their data. This raises the question of 'data portability' – whether individuals can move, copy or transfer their data from one IT environment or service provider to another. That could include transferring a playlist from one music streaming site to another, moving data from an energy utility to use in a carbon footprint calculator, or providing bank account history to a potential lender or an aggregator who can advise on personal finances.

Some competition experts argue that personal data portability encourages new market entrants, enables innovation, and enhances consumer welfare.[29] On the other hand, collecting, storing, protecting, and maintaining the integrity of sensitive personal data is costly. Portability could allow competitors to take advantage of this data at little cost, reducing the incentive for companies to invest in innovation. Companies could also suffer reputational damage or legal liability if a third party misuses the data.

Nonetheless, many customers are starting to expect data portability in some form. The current practice of 'screen scraping' in financial services in Canada – where millions of users have given third parties their bank login credentials to gather data for use in another service – raises significant privacy and security concerns. The question, then, is how to operationalize data portability in a way that is fair and secure.

Box 2: Regulatory approaches to consumer data portability

EU GDPR Data Portability: This is a fundamental new right enabling individuals to obtain a copy of their data in a structured, commonly used, and machine-readable format, as well as to have the data transmitted to another party without hindrance. The right pertains to data individuals have actively and knowingly provided, and to data provided indirectly, from using a website, search engine, or wearable device.

UK 'Open Banking': This is the first-ever practical implementation of personal data portability in a specific sector. It complies with GDPR and offers a complete framework for consumers and businesses to authorize third party financial service providers to access their financial transaction and direct payments data, using secure online channels. The UK Treasury proposed Open Banking in 2015 and the Competition and Market Authority ordered the nine largest retail banks to implement it in January 2018. To ensure privacy and security, the Financial Conduct Authority must authorize third-party participants.

Australia 'Consumer Data Right': Part of the *Data Sharing and Release Act*, this is a broad right for individual and business consumers to direct their service provider to share with them and others the digital information held about the consumer. The Australian Competition Commission will administer the new legislation. The right will first apply to banking, followed by utilities and telecommunications.

There are different models around the world. The EU, UK, and Australia have taken a regulatory approach, though they differ in the scope and detail of implementation (see Box 2). Australia and the EU, for example, have created an economy-wide legal right for consumers to port their data. The UK and Australia have combined this right with

sector-specific regulations, starting with banking, that mandate how data must be shared, and with whom. Australia plans to extend portability regulations into utilities and telecommunications, followed by other sectors.

There are also voluntary, or industry-led, approaches to data portability. In 2017, Facebook, Google, Microsoft and Twitter launched the Data Transfer project to allow users to move their data between multiple online and social media platforms. Consortiums of banks and health providers in the U.S. have also developed bilateral arrangements that allow clients to port their data between providers. Voluntary approaches, however, allow participants to exclude or set the terms for new entrants.

In Canada, there are proposals for both regulated and industry-led approaches to portability. The PIPEDA White Paper suggests a new general data portability right, building on the existing law's right to access, but ensuring that organizations use standardized formats and common approaches for transferring data. Finance Canada is currently exploring the merits of Open Banking, which includes a close look at the UK model.[30] A recent report on Open Banking from the Senate Committee on Banking Trade and Commerce recommended that PIPEDA include a consumer data right covering portability of financial data.[31] However, the report also suggests that Canada take an industry-led approach as a starting point.

Key questions:

- To what extent should consumers be able to move their personal data between different service providers?
- What is the best approach to facilitate data portability? Is regulation needed? If so, should it be sector-by-sector or economy-wide?

Business data rights

Business data rights are less defined than those of individuals. There are two main challenges: first, separating business data from personal data; and second, defining the commercial rights to data that are generated through industrial activities or in dealings with other businesses.

One way to address the first challenge is to consider business data simply as the non-personal data held by that organization. But it is hard to determine when data goes from personal information with privacy protections to non-personal data that can be freely used by an organization. Is it when the data is de-identified, anonymized, or aggregated? How should the insights or analytics built off personal data be treated? Ambiguity about these rights creates business uncertainty.

Other countries offer some guidance in this area. Australia does not consider 'imputed' data – data to which a company has applied insights or analysis – to be consumer data.[32] Similarly, data derived from combined sources, or data that cannot be re-identified, are not considered consumer data. Australia recommends that each industry work to define consumer data in more detail by undertaking a data specification process.

Recent EU guidance for GDPR offers specific examples of non-personal data. These include, for instance, data on travel that has been aggregated to hide a person's individual trips abroad, anonymous data used in statistics or in sales reports to assess the popularity of a product, and sector data such as high-frequency trading data in finance or data from precision farming.[33]

The second challenge is for business to protect and assert legal rights over purely commercial, or industrial data such as equipment maintenance records, 3D construction models, shipping details, or plant productions schedules. IP rights — including trade secrets, database rights, or copyright — can offer certain limited protections. But data rights are more typically defined on a case-by-case basis through the terms of commercial contracts. Companies lacking experience negotiating data rights may find themselves unable to access valuable data or locked into relationships with vendors. There is also a question of how to value these data rights in cases of acquisitions and bankruptcy proceedings.

The EU recently explored the issue of business data rights and found no need to create new ownership rights or other legislation to govern B2B data-sharing. However, the EU and Japan have considered promoting more transparency and consistency in how data is treated in commercial contracting through codes of conduct or the creation of standard contract terms.[34]

Key questions:

- Where should the line be drawn between personal and business data?
- Do businesses need more tools to assert and protect their rights to commercial or industrial data? Are contractual mechanisms enough?

3.3 Competition

An open marketplace supports privacy and consumer welfare as companies compete to offer their customers value and enhanced protection for their data. However, leading economists have raised concerns that data is being concentrated in the hands of a few firms and, therefore, limiting competition.[35] Commentators tend to focus on larger technology platforms, arguing that they can use data holdings to entrench market dominance and gatekeep the broader digital economy, excluding rivals, acquiring new entrants, and discriminating in favour of their own products and services.[36] But the same concern could apply to any market segment where access to data is a decisive competitive advantage.

Competition policy

Competition authorities are increasingly acting on data-related market issues. The German Federal Cartel Office has used anti-trust laws to restrict Facebook data collection policies. The U.S. Justice Department and Federal Trade Commission are both

looking into anti-trust issues involving large technology companies. The question is whether traditional competition enforcement approaches remain adequate.

As part of the *Digital Charter*, the government has asked the Competition Bureau to consider the impact of digital transformation on competition, including issues such as data accumulation, transparency, and control. The government also asked the Bureau to look at the effectiveness of current policy tools, marketplace frameworks, and investigative and judicial processes.

The Bureau's new Commissioner recommends modernizing enforcement tools to include increased fines, greater global coordination, and formal powers to undertake market studies.[37] Meanwhile, he appointed a new Chief Digital Enforcement Officer to help the Bureau monitor the digital landscape, identify and evaluate new investigative techniques, and gather intelligence.[38]

The UK is exploring expanded powers for its Competition and Markets Authority, specifically to deal with dominant companies. The Digital Competition Expert Panel recommends establishing a Digital Markets Unit to designate companies with 'strategic market status' and make them subject to a 'code of competitive conduct.'[39]

Other competition experts are urging caution. The C.D. Howe Institute's Competition Council, for instance, argues that Canada's Competition Bureau already has the powers it needs to handle new challenges. It warns about the potential negative impact new regulatory powers may have on investment, and the risk of dampening fast-moving competition 'for the market' in the technology sector.[40]

Key questions:

- Is data concentration hurting competition in Canada? In which sectors could this be a concern?
- Does the Competition Bureau have the mandate and tools to do its job?

Foreign investment policy

A recent report by the Public Policy Forum recommends that Canada screen foreign acquisitions of Canadian companies that hold valuable data or AI assets.[41] To do this more effectively, they propose two reforms to the *Investment Canada Act*. The first is a lower transaction threshold for review so that acquisitions of smaller technology companies would no longer be excluded. The second is an adjustment to the 'net benefits' criteria to require the government look into the impact of a transaction on data concentration. While these changes would give the government more tools to address competition concerns, such an approach could depress the valuations of Canadian technology companies and send a negative signal to foreign investors.

Key question:

- What is the impact of foreign acquisitions of data and AI companies on competition and innovation in Canada?

3.4 Public Sector Data

How governments collect and share data has implications for the data-driven economy. On the one hand, governments have exceptional powers to compel data from private individuals and businesses. On the other, they have valuable data that can help deliver better public services or that businesses can use to innovate and grow.

Government access to data

Governments need access to high-quality data to develop public policy, support regulatory activities, and deliver services to Canadians. This data is also used to generate statistics and data sets that businesses and consumers rely on for decision-making. For these reasons, federal laws give various agencies the power to compel data from citizens and businesses, subject to strict rules on privacy and confidentiality.

Finding the right balance can be difficult, however, as shown by last year's controversy over Statistics Canada's request for Canadian banks to provide certain customer financial data.[42] Under the *Statistics Act,* the agency may collect information through mandatory surveys and requests for administrative data from businesses. In this case, the agency was seeking information about the online spending habits of Canadians — important economic data that they have not been able to capture due to declining participation in traditional surveys.

However, the request generated public backlash and the banks refused to provide the data to Statistics Canada. Bank customers also lodged complaints under the *Privacy Act* – the law that governs how federal departments handle personal information – prompting the OPC to open an investigation into the issue. Statistics Canada subsequently withdrew its request.[43]

As part of the *Digital Charter*, the federal government announced it would review the *Statistics Act* to ensure confidence in how the agency gathers personal information.[44] The government is also planning to modernize the *Privacy Act*.[45] There may be potential for increased transparency around government data use, or notices when it intends to collect new data. Provinces may need to review their legislation in this area as well.

Key questions:

- What types of data are in the public interest?
- Under what terms should the government be able to compel access to private or confidential data? What process should governments follow?

Sharing public sector data

Greater sharing of public sector data can make government more transparent and accountable to citizens and generate value through the innovative use of that data by the private sector and research community.

The federal government has taken steps to make its data more available and accessible, but there are ongoing challenges. Canada joined the international Open Government Partnership at its launch in 2011 and produces a National Action Plan every two years.[46] The federal government's Open Data Portal now provides digital access to over 80,000 data sets.[47] Canada and the UK lead the world in the Global Open Data Index. But while the federal government gets good marks for transparency, industry engagement with the data has not met expectations. The focus now is on high-quality and high-value datasets, and how to provide them in developer-friendly formats, with real-time data updates, common communication formats, and better standards for server uptime.

To be more systematic about data release, federal departments need to modernize how they govern their data. Last year, the Treasury Board Secretariat, which sets rules for department IT practices, and the Privy Council Office, a central agency, released a Data Strategy Roadmap for the federal public service. It lays out a whole-of-government approach to internal data policies and establishes a senior level decision-making body, as well as a Chief Data Steward.[48] All departments, and agencies must develop data strategies and put in place frameworks and standards for ethical and secure use and sharing of data.

Governments in other countries are also moving towards more systematic approaches to data release. The EU has recently updated their Directive on Open Data and Public Sector Information, calling on member states to make greater efforts to identify and release high-value datasets with significant commercial potential, such as statistics or geospatial data. Australia has appointed a National Data Commissioner and created the concept of 'National Interest Data Sets' that the government should prioritize.[49]

The goal for many governments is to eventually make data open by default. The new EU Directive aims to make all public sector content covered by national access to information rules, in principle, freely available for re-use. In a recent review of public sector practices, Australia concluded that data not specifically relating to individuals or businesses, and not subject to intellectual property rights, should routinely be made available.[50]

Realizing the full potential of government data-sharing may require legislative changes. Australia is consulting on a new *Data Sharing and Release Act*, for instance, that would streamline regulations and mitigate risks that currently impede departments from sharing and releasing data. Among other things, it would provide a risk-based approach to authorizing sharing and release, clarify the roles of 'data custodians', and establish trusted 'end-users'.[51] Canada should evaluate this model as it modernizes the *Privacy Act* and *Statistics Act.*

Key questions:

- Is Canada doing enough to release valuable public data sets? How should governments prioritize data for release? What are the barriers?
- On what terms should private companies be able to access public data? Who should cover the costs?

3.5 Cross-border Data Flows

Since its founding, a basic premise of the Internet has been the free flow of data and information around the world. Cloud computing has accelerated the trend, as it allows organizations to leverage storage and computing infrastructure from around the world. But this global integration is coming under strain. In pursuit of various public policy goals, governments are establishing local storage and processing requirements, controls on cross-border data flows, and a patchwork of different, and sometimes contradictory rules that organizations must follow. Some warn of a 'splinternet', where national governments, knowingly or unknowingly, carve up cyberspace to the detriment of a free and open Internet.[52] Canada has important decisions about its own policies, how it coordinates with the provinces, and how it tries to influence international frameworks and norms to Canada's advantage.

Data localization and rules on cross-border flows

Just as governments traditionally regulate the flow of people, capital, and goods across their borders, they are starting to exert more control over international data flows. They do so for a variety of stated and unstated reasons. Governments may, for instance, want to ensure data access for local law enforcement or regulators, stimulate the local technology sector, or protect against other governments or organizations from accessing sensitive data.

Regulations on cross-border flows can be put in two main groups. The first and most restrictive type require that organizations store and process data locally. China and Russia, for instance, make extensive use of such measures. Measures in the second group are more flexible. They allow organizations to move data across borders but require them to maintain certain standards of data access, treatment, or protection wherever they locate the data. Depending on how they are implemented, governments can use this latter type of measure to achieve their public policy objectives without significantly impacting cross-border flows.

How a country approaches cross-border data flows has significant economic implications, as it can make it harder for local firms to take advantage of cloud computing solutions. A 2017 industry study, for instance, found that countries with data localization and other impediments to cross-border data flows have higher IT costs and lower GDP.[53]

Currently in Canada, federal and provincial governments require some types of data to be stored and processed locally. Nova Scotia and British Columbia, for instance, require most government-held personal data to be stored on local servers. Another example is the federal Office of the Superintendent of Financial Institutions, which can require financial institutions to store certain accounting data locally in order to facilitate access in case of a banking crisis. These policies continue to evolve. A recent paper from the Treasury Board of Canada says that Canada is 'following other lead of other countries' to

limit the categories of government-held data that can be stored in the cloud. One of their concerns is that the U.S. government could compel service providers to turn over sensitive Canadian data under the Foreign Intelligence and Surveillance Act.[54]

More generally, however, Canada's policies support cross-border data flows. PIPEDA, for instance, does not prohibit organizations from transferring information outside Canada. It does require them, however, to apply the same level of privacy and data protection abroad as they would in Canada, regardless of local laws.

In a controversial move, the OPC recently suggested that Canadian organizations may also need individuals to consent to cross-border transfers of personal information. This break from longstanding practice stems from their findings on the recent Equifax data breach case, which reinterpreted PIPEDA obligations. The OPC has launched consultations to consider a new guideline expanding on this interpretation.[55] This position would cause major disruptions to IT arrangements and is highly contested by industry and the legal community.

The EU has strict rules on cross-border flows of personal data, though they do not require organizations to get individual consent. Personal data can flow freely to third countries that have comparable privacy laws to the EU. The European Commission maintains a list of third countries that it deems to offer 'adequate' protections. For countries that are not on that list, including the U.S., the EU allows organizations to transfer data using standard model clauses or binding corporate rules approved by EU or national authorities. As a last resort, organizations can use individual consent.

Key questions:

- How are local storage requirements impacting data-driven innovation in Canada?
- Are there cases in which data localization is necessary for the public interest?
- What requirements should businesses have to meet when storing and processing sensitive data abroad?

Regulatory coordination

The proliferation of different data rules around the world, and even within Canada, have created a patchwork that imposes costs on business and limits cross-border data flows. As Canada modernizes its data laws, the federal government will need to make them interoperable with provinces and international trade partners.

The European Union has taken the lead in setting global privacy rules. Part of the rationale for GDPR, for instance, was to create one common, high-quality framework for privacy protections across the EU, harmonizing national laws and eliminating barriers to cross-border data flows. Internationally, many countries are following its lead. From California to China, there seems to be a growing convergence on the EU model.[56]

Canada may also have an incentive to align its privacy reforms with the EU. Currently, Canada is one of eleven non-EU countries on the European Commission's adequacy list, though that status was granted before the latest updates to GDPR. Canada will be up for

review again in 2020. With the newer rules, Canada may need to reorient some elements of its privacy laws to maintain alignment. Adequacy, however, does not require equivalence, which means that Canada can still have its own distinct approach.

Within Canada, data privacy is a shared jurisdiction. British Columbia, Alberta, and Quebec have their own general laws for how business handles personal data, which the federal government considers to be equivalent to PIPEDA. Moreover, most provincial have specific laws regulating personal data in health care, education, and employment – areas of significant economic potential. These rules differ and are constantly changing, making it difficult for organizations to work with this data at a national level. Ontario, for instance, recently launched its own data strategy consultations, which may create yet more unique obligations.[57]

Key questions:

- To what extent should Canada align its privacy laws to those of other jurisdictions, such as the EU?
- How can we better align data rules between the federal and provincial governments? In which sectors is alignment needed the most?

International agreements and norms

Treaties and other forms of international cooperation can help align regulations, build trust, and reduce barriers to cross-border data flows.

Modern free trade agreements increasingly address cross-border data flows. The Trans-Pacific Partnership (TPP) and Canada-U.S.-Mexico Agreement (CUSMA), for instance, have enforceable provisions against data localization and restrictions on cross-border flows, preventing countries from imposing them for protectionist purposes. Many countries are proposing that similar provisions be negotiated in new digital trade and services agreements at the World Trade Organization. Although the TPP and CUSMA have exceptions that permit countries to regulate cross-border flows to protect privacy and other public objectives, some argue that Canada should not be making any commitments that tie its hands, especially when the digital landscape is evolving so quickly.[58]

Canada is active in several regional and multilateral forums that seek to align data rules on privacy. Rather than bind countries through treaties, governments develop common approaches and templates to follow. The OECD Guidelines on Privacy and Transborder Data Flows, for instance, first issued in 1980 and updated in 2013, have shaped many national privacy laws, including Canada's. Canada is also an early member of the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules system. This body brings non-OECD countries into the fold to develop globally interoperable privacy laws.

More recently, Canada has been trying to shape global norms around AI governance. At last year's G7 summit in Quebec, Canada established an International Panel on AI with France, with hopes that other countries would join the initiative.[59] At this year's G20

summit in Japan, countries endorsed the OECD's new Ethics and AI guidelines.[60] Japan had put global data governance at the top of the agenda in the belief that countries need to build trust with each other to remain open to international data flows.

Key questions:

- How should free trade agreements address cross-border data flows?
- Which forums should Canada use to influence global norms around data and AI governance?

3.6 Data Infrastructure

A data-driven economy needs common mechanisms or data 'infrastructure' to securely and efficiently collect, share, and integrate data. This may include standardized communications formats and data governance practices, as well as institutions that can help manage common datasets. Internationally, such infrastructure has been necessary to operationalize new policy frameworks on privacy, portability, and open access. Industry and government need to consider how this infrastructure is governed and financed.

Standards, codes of conduct, and certification

Formalizing the ways organizations communicate and govern data can make it easier to share, foster trust, and support compliance with domestic and international regulations. On the other hand, standards are costly to develop and implement, can impact competition, and cause companies to focus on meeting certain rules, instead of the underlying objectives.

Organizations are increasingly standardizing communications formats. This is done using Application Programming Interfaces (or 'APIs') that allow different software and databases to exchange messages or data in a common way. When a customer books airline seats on Expedia, for instance, they choose departure and return dates, cabin and budget preferences, and the site returns the options. Expedia does not have direct access to the airline databases; rather, it interacts with the various airline APIs.

Data portability typically requires APIs. In the case of the UK and Australia, their governments mandate that companies develop and use common APIs so that consumers can seamlessly move their data between different service providers (see Box 3). In Canada, a consortium of banks is collaborating with SecureKey on a digital identity platform using blockchain technology that makes it easier for individuals to confirm their identities and login to different service providers.[61] There may be opportunities in other industries to develop common APIs.

Data governance standards, on the other hand, are broader than APIs, and can build trust between entities that the data they share is secure and accurate. This is particularly important with sensitive data, such as health records, where a breach or inaccuracy could cause serious harm. Data governance standards may cover how data is

stored, archived, and backed up; how it must be protected from mishaps, theft or attacks; how permissions are issued to authorized personnel; and how to demonstrate compliance with government regulations.

Several Canadian initiatives to standardize data governance are underway, though industry engagement to date has been somewhat limited. As part of the *Digital Charter*, the Standards Council of Canada (SCC) recently launched the 'Canadian Data Governance Standardization Collaborative'. This group is developing a comprehensive roadmap of data governance standards across industries and will identify gaps that Canada can fill.[62] Already, the CIO Strategy Council, accredited by the SCC, is drafting a standard for data access and privacy, as well as for the ethical use of data and AI.[63] Another example is Ryerson University's certification scheme for a 'Privacy by Design' framework. This made-in-Canada standard is being drafted into a global standard through the International Standards Organization.[64]

Canada could take a more active role in other international standardization initiatives. The Industrial Internet Consortium, for instance, brings together the world's leading technology companies in the industrial Internet space, with the aim of driving interoperability.

Government can support data governance standards by recognizing them in legislation and regulation. The PIPEDA White Paper, for instance, suggests the law or the department name specific industry data privacy standards or codes to incentivize company adoption. The Canadian Marketing Association, for instance, has a Code of Ethics and Standards of Practice. The government would consider these codes, standards, and certifications as proof of compliance with privacy rules, or as a mitigating factor in cases of investigations.

Box 3: Standards for data portability

UK Open Banking Implementation Entity: The UK Treasury commissioned a Working Group to create the Open Banking Standard in 2015. A group of 150 expert participants working across six subgroups from 80 different organizations collaborated on the Standard. In addition to providing technical guidance on the API, the Standard considers a broad range of issues: governance, security, liability, regulatory and legal, and communications. The Open Banking Implementation Entity made the Standard the basis of the marketplace framework they introduced in January 2018. All UK work on the Standard is freely available through open licenses.

Australia Data Standards Body: Australia created a new Data Standards Body to carry out the work for their new Consumer Data Right, with industry and consumer advice provided by an Advisory Committee. The government appointed Data 61, an innovation group, as a technical advisor to design the first iteration of open technical standards that would support APIs for consumer-driven data-sharing. As a starting point, Australia used the work of the UK Standard for Open Banking.

Key Questions:

- Would Canadian industry benefit from more common APIs and data governance standards? If so, in what areas?

- Should the government formally recognize industry codes, standards, or certifications?

Data libraries and trusts

Earlier this year, the federal government's Economic Strategy Tables, made up of business leaders from six top Canadian sectors, recommended that the government help create industry data platforms and 'big data libraries'. Companies would pool large quantities of anonymized data, giving innovators testbeds to develop sector-specific AI or other data analytics solutions.[65] These could be housed in Canada's five Supercluster initiatives, which are generating significant sector-specific data. To be interoperable, companies would need to agree on how the data is defined, structured, and represented both internally and externally.

For sensitive data, some have proposed the creation of 'data trusts' that use an independent institution with trustees to make decisions about how data is collected, used, and shared. In addition to protecting the data, trusts can be used to ensure that competitors have common levels of access. Sidewalk Labs, for example, has included a variation of this model as part of its proposal for Waterfront Toronto's Quayside project in Toronto. The proposal calls for the creation of an independent, government sanctioned 'Urban Data Trust' that would review and approve proposed collections and uses of data collected in physical spaces such as the public realm and publicly accessible spaces. The Urban Data Trust would provide additional privacy protections for personal information and make non-personal and aggregate data publicly available by default.".[66]

The PIPEDA White Paper proposes data trusts as a way for organizations to share and process de-identified personal information in a safe and responsible manner, eliminating the need for organizations to seek individual consent. It sees applications for public-private partnerships in areas such as health or transportation, and a role for government in laying out the governance framework. The concept of data trusts is still relatively new and building one is not an easy or well-understood task.[67] It is not yet clear what the appropriate funding model is and how trustees should be selected.

Key questions:

- Which sectors of the economy would benefit from pooling their data? What role should government play in this?
- Are data trusts a solution to manage access to, and use of, sensitive data? How should they be governed and who should pay for them?

---

[1] Desjardins, J. (2019, April 17). How much data is generated each day? Retrieved from https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

[2] Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., . . . Trench, M. (2017, June). Artificial Intelligence: the Next Digital Frontier? Retrieved from https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced Electronics/Our Insights/How artificial intelligence can deliver real value to companies/MGI-Artificial-Intelligence-Discussion-paper.ashx

[3] Manyika, J, Bughin, J, Lund, S, Nottebhom, O., Poulter, D., Jauch, S., . . . (2014, April). Global flows in a digital age. Retrieved from https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age
[4] Statistics Canada. (2019, July 10). The value of data in Canada: Experimental estimates. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/190710/dq190710a-eng.htm.
[5] Haskel, J., & Westlake, S. (2017). *Capitalism without Capital: The Rise of the Intangibles Economy.* New Jersey: Princeton University Press.
[6] Agrawal, Ajay; Joshua Gans; and Avi Goldfarb. (2018). *Prediction Machines: The Simple Economics of AI*. Boston: Harvard Business Review, p215-17.
[7] Statistics Canada. (2019, July 10).
[8] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015, June). Unlocking the potential of the Internet of Things. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
[9] Bughin, J. et al. (2017, June).
[10] Agrawal, Ajay et al. (2018). p16-17.
[11] Centre for International Governance Innovation, (2018, February). A National Data Strategy for Canada: Key Elements and Policy Considerations. CIGI Papers No. 160.
[12] Government of Canada. (2019, July 21). Canada's Digital Charter in Action: A Plan by Canadians, for Canadians. Retrieved from https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html
[13] Harris, P. (2018, July 4). Data, the European Union General Data Protection Regulation (GDPR) and Australia's New Consumer Right. Speech. Retrieved from https://www.pc.gov.au/news-media/speeches/data-protection
[14] Office of the Privacy Commissioner of Canada. (2019, May 09). 2018-19 Survey of Canadians on Privacy. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/#toc1
[15] Cobb, S. (2018). ESET Cybersecurity Barometer Canada. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2019/01/ESET_BAROMETER_USA.pdf
[16] House of Commons Standing Committee on Access to Information, Privacy and Ethics. (2018, February 28). Review of the *Personal Information Protection and Electronic Documents Act*. Retrieved from https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=9213226
[17] Government of Canada. (2019, May 21). Strengthening Privacy for the Digital Age: Proposals to Modernize the *Personal Information Protection and Electronic Documents Act*. Retrieved from https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html
[18] Coleman, J (2018, May 23). Here's How Long It Would Take to Read All the New Privacy Updates. Retrieved from https://medium.com/@jnameloc/heres-how-long-it-would-take-to-read-all-the-privacy-updates-you-ve-been-getting-cd4f215cff6d
[19] Meyer, D. (2018, October 10). Amazon Reportedly Killed an AI Recruitment System Because It Couldn't Stop the Tool from Discriminating Against Women. Fortune. Retrieved from https://fortune.com/2018/10/10/amazon-ai-recruitment-bias-women-sexist/
[20] Treasury Board of Canada Secretariat. (2017, August 24). Directive on Automated Decision-Making. Retrieved from https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592
[21] Office of the Privacy Commissioner of Canada. (2018, October 10). Announcement: Privacy Commissioner seeks Federal Court determination on key issue for Canadians' online reputation. Retrieved from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181010/
[22] Low, J. (2018, April 20). The 'right to be forgotten' poses unacceptable risks to freedom of expression. Canadian Journalist for Free Expression. Retrieved from https://www.cjfe.org/the_right_to_be_forgotten
[23] House of Commons Standing Committee on Access to Information, Privacy and Ethics. (2018, February 28). Democracy under threat: risks and solutions in the era of disinformation and data monopoly. Retrieved from https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf; and Office of the Privacy Commissioner of Canada. (2018, November 23). National Digital and Data Consultations. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ised_181123/
[24] Information Commissioner's Office. (2019, July 9). Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach. Retrieved from https://ico.org.uk/about-the-

ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/
[25] Information Commissioner's Office. (2019, July 08). Intention to fine British Airways £183.39m under GDPR for data breach. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
[26] Public Safety Canada. (2018). *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age.*
[27] House of Commons Standing Committee on Public Safety and National Security. (2019, June). Cyber security in the financial sector as a national security issue. Retrieved from https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf
[28] Obama White House Archives. Using Cyber-Insurance to Improve Cyber-Security: Legislative Solutions for the Insurance Market. Retrieved from https://obamawhitehouse.archives.gov/files/documents/cyber/ISA - Cyber-Insurance Metrics and Impact on Cyber-Security.pdf
[29] HM Treasury. (2019, March 13). Unlocking Digital Competition: Report of the Digital Competition Expert Panel. Retrieved from https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel
[30] Finance Canada. (2019, January 11). A Review into the Merits of Open Banking. Retrieved from https://www.fin.gc.ca/activty/consult/2019/ob-bo/obbo-report-rapport-eng.asp
[31] Standing Senate Committee on Banking, Trade and Commerce. (2019, June). Open Banking: What it Means for You. Retrieved from https://www.sencanada.ca/en/info-page/parl-42-1/banc-open-banking/
[32] Productivity Commission. (2017, March 31). Productivity Commission Inquiry Report: Overview and Recommendations. Data Availability and Use. Retrieved from https://www.pc.gov.au/inquiries/completed/data-access/report
[33] European Commission. (2019, May 29). Commission publishes guidance on free flow of non-personal data. Digital Single Market. Retrieved from https://ec.europa.eu/digital-single-market/en/news/commission-publishes-guidance-free-flow-non-personal-data.
[34] Ibid.
[35] Wilkins, C. (2018, February 8). At the Crossroads: Innovation and Inclusive Growth. Speech. Retrieved from https://www.bankofcanada.ca/2018/02/crossroads-innovation-inclusive-growth/; and
HM Treasury. (2019, March 13). Unlocking digital competition, Report of the Digital Competition Expert Panel. Retrieved from https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel
[36] Competition Bureau Canada. (2019, June 13). Competition in the Age of the Digital Giant. Retrieved from https://www.canada.ca/en/competition-bureau/news/2019/06/competition-in-the-age-of-the-digital-giant.html
[37] Thérien, D., St-Jean, S., & Annie, B. (2019, June 19). The New Commissioner of Competition Requests Changes to Address Digital Economy Challenges. Retrieved from http://www.mondaq.com/canada/x/816628/Data+Protection+Privacy/The+New+Commissioner+Of+Competition+Requests+Changes+To+Address+Digital+Economy+Challenges
[38] Competition Bureau Canada. (2019, July 02). George McDonald joins the Competition Bureau as new Chief Digital Enforcement Officer. Retrieved from https://www.canada.ca/en/competition-bureau/news/2019/07/george-mcdonald-joins-the-competition-bureau-as-new-chief-digital-enforcement-officer.html
[39] HM Treasury. (2019, March 13).
[40] C.D. Howe. (2019, May 16). Competition Bureau already has the "Toolkit" to Handle Big Tech: C.D. Howe Institute Competition Policy Council. Retrieved from https://www.cdhowe.org/cpc-communique/competition-bureau-already-has- "toolkit"-handle-big-tech-cd-howe-institute-competition-policy
[41] Asselin, R., & Speer, S. (April 2019). A New North Star: Canadian Competitiveness in an Intangible Economy. Public Policy Forum. Retrieved from https://ppforum.ca/wp-content/uploads/2019/04/PPF-NewNorthStar-EN4.pdf.
[42] Curry, B. (2018, November 04). Controversy over Statscan's plan to obtain personal banking records exposes problems with current data. Retrieved November 4, 2018, from

https://www.theglobeandmail.com/politics/article-controversy-over-statscans-plan-to-obtain-personal-banking-records/
[43] Office of the Privacy Commissioner of Canada. (2018, October 31). Announcement: Privacy Commissioner launches investigation into Statistics Canada. Retrieved from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181031/
[44] Canadian Press. (2019, May 21). Minister Bains outlines digital charter with focus on personal data control. Retrieved from https://www.ctvnews.ca/politics/minister-bains-outlines-digital-charter-with-focus-on-personal-data-control-1.4430952
[45] Department of Justice. (2019, May 22). Modernizing Canada's *Privacy Act*. Retrieved from https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html
[46] Treasury Board Secretariat of Canada. (2019, July 15). Canada's 2018-2020 National Action Plan on Open Government. Retrieved from https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government
[47] Treasury Board Secretariat of Canada. (2019, March 01). Open Data in Canada: A look at the Numbers. Retrieved from https://open.canada.ca/en/blog/open-data-canada-look-numbers
[48] Government of Canada. (2019, April 11). Report to the Clerk of Privy Council: A Data Strategy Roadmap for federal public service. Retrieved from https://www.canada.ca/en/privy-council/corporate/clerk/publications/data-strategy.html
[49] Office of the National Data Commissioner. (2018). National Data Commissioner. Retrieved from https://www.datacommissioner.gov.au/
[50] Australian Government (2018, July 25). Review of Australian Government Data Activities 2018. Retrieved from https://www.pmc.gov.au/resource-centre/public-data/review-australian-government-data-activities-2018
[51] Flannery, A. (2019, January 17). Public sector data, the proposed Data Sharing and Release Act and implications for governments. Retrieved from http://www.mondaq.com/australia/x/772966/Constitutional+Administrative+Law/Public+sector+data+the+proposed+Data+Sharing+and+Release+Act+and+implications+for+governments
[52] Wright, K. (2019, March). The 'splinternet' is already here. Techcrunch. Retrieved from https://techcrunch.com/2019/03/13/the-splinternet-is-already-here/
[53] Cory, N. (2017, May 1). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation. Retrieved from https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost
[54] Treasury Board of Canada Secretariat. (2018, May 25). Government of Canada White Paper: Data Sovereignty and Public Cloud. Retrieved from http://publications.gc.ca/collections/collection_2018/sct-tbs/BT22-213-2018-eng.pdf
[55] Office of the Privacy Commissioner of Canada. (2019, June 11). Consultation on transfers for processing – Reframed discussion document. Retrieved from https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/
[56] Sacks, S. (2018, March 9). China's Emerging Data Privacy System and GDPR. https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr
[57] Government of Ontario. (2019, February 5). Ontario's Government Launches Data Strategy Consultations. Retrieved from https://news.ontario.ca/mgs/en/2019/02/ontarios-government-launches-data-strategy-consultations.html
[58] Ciuriak, D. (2018, February). "Digital Trade: Is Data Treaty-Ready?" CIGI Papers No. 162. Retrieved from https://www.cigionline.org/sites/default/files/documents/Paper%20no.162web.pdf
[59] Innovation, Science, and Economic Development Canada. (2019, May 16). Canada and France work with international community to support responsible use of artificial intelligence. Retrieved from https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/canada-and-france-work-with-international-community-to-support-responsible-use-of-artificial-intelligence.html
[60] OECD. (2019, May 22). Forty-two countries adopt new OECD Principles on Artificial Intelligence. Retrieved from https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm
[61] SecureKey Technologies Inc. (2019, May 1). SecureKey and Initial Network Participants Accomplish Key Milestone in Bringing Digital Identity Network to Market. (n.d.). Retrieved from https://securekey.com/press-releases/verifiedme-launch-release/

[62] Standards Council of Canada. (2019, May 21). Using standards to power a data-driven economy. Retrieved from https://www.scc.ca/en/news-events/news/2019/canadian-data-governance-standardization-collaborative
[63] CIO Strategy Council. (2019, June 5). New Projects. Retrieved from https://ciostrategycouncil.com/standards/new-projects/
[64] Standards Council of Canada. (2018, December 3). Canada leading the way on privacy-by-design standard. Retrieved from https://www.scc.ca/en/news-events/news/2018/canada-leading-way-privacy-design-standard
[65] Innovation, Science and Economic Development Canada. (2018, September 28). Report from Canada's Economic Strategy Tables: Digital Industries. Retrieved from https://www.ic.gc.ca/eic/site/098.nsf/eng/00024.html
[66] Sidewalk Labs. (2018, October). Digital Governance Proposals for DSAP Consultation. Retrieved from https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft Proposals Regarding Data Use and Governance.pdf?MOD=AJPERES
[67] Open Data Institute. (2019). Data Trust summary report. Retrieved from https://theodi.org/wp-content/uploads/2019/04/ODI-Data-Trusts-A4-Report-web-version.pdf