Data Driven

Canada's economic opportunity

THEBUSINESSCOUNCIL.CA

Business Council
of Canada

Data Driven

Canada’s economic opportunity

Contents

Executive Summary

Data is transforming Canada's economy and society. Advances in digital technology allow people and organizations to gather and store ever more data, enabling smarter and faster decisions that fuel innovation, contribute to economic growth, and improve the lives of citizens.

Digital transformation also gives rise to significant new public policy questions. How can Canadians and their institutions collect and make use of data while safeguarding privacy, security, and rights? How do we ensure that new laws and regulations do not impede important and beneficial new technologies and services? How can we enable consumers to protect their data without sacrificing convenience or user experience? How do we leverage our country's talents and strengths to harness the power of digital and data transformation?

Countries and jurisdictions around the world are attempting to realize the opportunities and address the challenges of a data-driven world. Canada can be a leader in this area, but we must move quickly. The stakes are high, and we cannot afford to get it wrong. To put it in perspective, Statistics Canada estimates that Canadians invested as much as $40 billion during 2018 in data, databases and data science. That was greater than the total investment that year in industrial machinery, transportation equipment, and research and development.

In May 2019, the federal government announced a new *Digital Charter*, a set of cross-cutting principles that will guide reforms to key legislation such as the *Personal Information Protection and Electronic Documents Act*, the *Privacy Act*, the *Competition Act* and the *Statistics Act*.

This report responds to the government's request for input by putting forward 24 recommendations that address three broad priorities: protecting Canadians, supporting a competitive marketplace, and building data infrastructure. Our work began with the development of an issues paper in the early summer of 2019. We then established an advisory panel of technology executives and former regulators. Led by The Honourable James Moore, former federal Minister of Industry, the advisory panel consulted dozens of leading Canadian companies across the country in a wide variety of industries.

All who took part in our consultations agreed that the emerging data economy offers significant benefits to consumers, industry and Canada as a whole. Examples range from improved healthcare outcomes, transportation networks, and government services, to more efficient energy use and farming practices.

At the same time, participants agreed on the need to modernize Canada's policy frameworks to take account of the growing importance of data in the economy and society. In certain areas, we found consensus on detailed recommendations. In others, we were only able to arrive at general recommendations. These areas will require further work to better understand the issues and policy options, and to bridge diverging viewpoints.

> **Canada will not reap the benefits of the digital revolution unless citizens have confidence that their privacy is protected and their data is not being misused. Building this foundation of trust requires a policy framework that ensures high levels of data protection.**

We believe there is both a need and an opportunity to develop a made-in-Canada approach to federal data policy – one that strikes an appropriate balance between market forces and regulation, that aligns with policies adopted by the provinces and our major trading partners, and that enables the private sector to innovate in ways that are responsible and beneficial to consumers and society.

Protecting Canadians

Canada will not reap the benefits of the digital revolution unless citizens have confidence that their privacy is protected and their data is not being misused. Building this foundation of trust requires a policy framework that ensures high levels of data protection.

Canada was an early leader in privacy law, but the world has changed since the drafting of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in the late 1990s. There is ample room to modernize and strengthen Canada's policy frameworks in ways that will enable individuals and companies to better protect their data from potential harms – including accidental release, fraud, theft, unauthorized access, and inappropriate use.

Our consultations identified several areas for improvement, and we offer recommendations dealing with consent and transparency, automated decision-making and algorithms, the right to be forgotten, enforcement and cybersecurity.

Supporting a competitive marketplace

Canada's policy framework also needs to enable and encourage the legitimate sharing and exchange of data. Today, this is sometimes difficult. Data is not owned in the traditional legal sense. On a technical level, it is often locked in silos and difficult to access. To a growing extent, data is becoming concentrated in the hands of a few key players, causing imbalances in market power. There are also growing barriers to the flow of data across domestic and international borders.

The push to create new market frameworks for data can be seen in the trend towards consumer data portability, the right of individuals to access personal data held by one organization and move it to another. Regulations need to support business data rights, and competition policy needs updating, to enable appropriate flows of data within Canada and abroad.

Our proposals in this area address individual rights to data portability in a digital format through robust and uniform frameworks, an expanded role for the Competition Bureau, and the need for harmonization of data strategies and policies at the federal and provincial levels.

Building data infrastructure

A data-driven economy also needs common data infrastructure. That includes codes, standards, and common mechanisms, practices, as well as institutions to securely and efficiently collect, share, and integrate data.

The federal government can help to develop this shared infrastructure through public investment, industry coordination, the adoption of enabling regulation, and by making its own data available to the private sector. The federal government must also support data and digital literacy among individuals, businesses of all sizes, and within government itself. And it must be mindful of provincial jurisdiction over key elements of the digital ecosystem.

Our recommendations support the development of voluntary codes of conduct and industry standards for data governance – currently a fragmented and incomplete landscape – as well as measures to bridge the gap between general regulatory obligations and specific data management practices.

Introduction

Data is transforming our economy and society. Advances in digital technology allow organizations of all kinds to gather and store ever more data, enabling smarter and faster decisions that increase productivity, contribute to economic growth and improve our lives. But these rapid advances also bring new challenges and raise important questions for public policy. How can Canadians and their governments protect privacy and cybersecurity while ensuring the optimal conditions for competition and innovation in a data-driven economy?

Canada has access to homegrown and international data science talent, but ideas and investment will ultimately go where they are most wanted and needed. The global race is fierce, and many other jurisdictions are making smarter, faster improvements to their data policy frameworks.

The public policy questions are wide-ranging and involve a broad range of stakeholders, including consumers, citizens, communities, industry and government. This report tries to answer these questions from the perspective of Canadian employers and innovators. It is the result of a Business Council of Canada research initiative aimed at developing consensus on recommendations to modernize Canada's data policy frameworks and ensure Canada's success in a data-driven world.

We began by asking The Honourable James Moore, former Minister of Industry, to chair an advisory panel of technology executives and former regulators. Following the release of an issues paper in July, the panel gathered input from dozens of leading Canadian companies in industries and regions across the country. (See Appendix.)

Without exception, Canadian companies regard the emerging data-driven economy as an enormous opportunity to grow and compete globally. Data is helping them run their businesses better, collaborate with partners, and create value for their customers. But they also see challenges – including a critical need for government policy to keep up with these transformational changes.

This report outlines recommendations for the federal government and business in three areas: protecting Canadians, supporting a competitive marketplace, and building data infrastructure.

In certain areas, the study found consensus on detailed recommendations. In others, it was only able to arrive at general recommendations. These areas will require further work with industry, government and other stakeholders to better understand the issues and policy options, and to bridge diverging viewpoints.

The body of this report consists four sections. First, it reviews the rise of data as a vital economic resource and explores how governments, here and around the world, are responding. Second, it outlines the key opportunities for Canada. Third, it summarizes the challenges businesses face in realizing these opportunities. Finally, it offers recommendations for how Canada can unlock the value of data in ways that benefit citizens and society, while respecting the rights of all stakeholders.

The rise of data

The speed with which data is generated today is unprecedented. We generate data every time we make a purchase, visit a website or use a connected device to communicate.

The volume of industrial data is also exploding. The Internet of Things (IoT) is dramatically increasing the number of devices that gather and share data. The advent of 5G wireless networks will accelerate this trend across all aspects of industry and society.

Advances in cloud computing, processing power, artificial intelligence (AI), and data science enable us to turn raw data into new insights and to make better predictions about the world around us. The applications are endless. Data can help commuters save valuable travel time, tell farmers where and when to plant seeds to ensure higher yields, or enable mental health workers to deliver services to patients who are most in need.

McKinsey estimates that AI will drive changes that 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. It is this economic potential that is driving demand for data and turning it into such a highly prized asset for organizations of all kinds.

But the economic properties of data are unlike those of other assets. In their book "Capitalism without Capital: The Rise of the Intangible Economy", Jonathan Haskel and Stian Westlake outline four key ways in which investments in data, or intangible assets, differ from investments in traditional tangible assets such as machinery or buildings:

- Synergies. Intangible investments tend to be more valuable together in the right combinations. The more information you have, the more value can be extracted.
- Scalability. Intangible assets can be used repeatedly and in multiple places at the same time.
- Spillovers. When you build a factory, it is yours to use. When you invest in ideas and information, it is more difficult to stop others from taking advantage of it.
- Sunk costs. If you no longer need your factory, you can sell it. In contrast, there is often little you can do to recover your money if your investment in data fails to generate a return.

These unique properties make returns on data investment less certain and more likely to be contested by others. As a result, some companies will choose to underinvest in these assets, while those that do invest can quickly become dominant. In such winner-take-all markets, companies that already have a lot of data or an advantage in AI have an incentive to invest further in these assets, while others fall behind.

These dynamics require new approaches to economic policy. The tangibles economy has a long history of institutions and norms: property rights, market pricing, standards, and regulations that have proven adaptable over time. The economic model for data is less well developed and understood, potentially giving rise to market failures.

The situation is further complicated by the fact that there are many types of data. We all have our own personal information, such as health records, banking history or email archives. Companies have their own confidential data, including sales numbers and the data they collect from sensors on equipment or production lines. Some data is publicly available from statistical agencies, web searches or other sources. Organizations can also use aggregation, analytics or AI to turn raw data into new forms of data such as customer profiles or weather predictions. Different contexts for data collection and use require different policy treatments.

Governments are responding

Governments around the world are seeking to establish marketplace rules and norms that will drive competition and encourage investment in data-driven innovation. But they also need to address a wide range of social and political risks. There are concerns about how the collection and use of personal data affects individuals, whether through surveillance and monitoring, bias in employment decisions or voter manipulation. Military strength increasingly depends on data and AI, while increasing reliance on industrial data to manage critical infrastructure is creating new cyber vulnerabilities.

To tackle this cluster of issues, many countries have launched cross-cutting national data strategies. Singapore was an early mover, launching its “Smart Nation” strategy in 2014. In 2016, Australia commissioned a study to expand the availability and use of private- and public-sector data, leading to significant reforms to the legislation that governs how consumers, business, and government access and share data. More recently, the United Kingdom launched its own National Data Strategy, building on the country’s pioneering work in the area of open government.

Some of the biggest changes have come in the area of privacy. The European Union’s General Data Protection Regulation (GDPR) came into effect in in 2018. California, too, has passed new legislation. Some U.S. lawmakers and technology companies are now pushing for federal legislation. China enacted its own Internet Security Law in 2016.

Canada has big decisions to make

Canada can continue to be an innovator in the data-driven world, but it must move fast. Our country has an enviable reputation for AI research and a strong privacy regime. The challenge now is to learn from others and build on our strengths to ensure that Canada remains an attractive location for responsible data-driven innovation.

The work has already started. Last May, the federal government unveiled its *Digital Charter,* which outlines a set of high-level principles that aim to modernize Canada’s data frameworks. As part of this exercise, the government is reviewing key federal laws, including PIPEDA, the *Privacy Act*, the *Competition Act* and the *Statistics Act*.

As the federal government modernizes these frameworks, it needs to strike an appropriate balance among regulation, market forces, competition policy and the needs of statisticians and researchers. Coordination among levels of government will be important. Provinces have constitutional jurisdiction over property and civil law, and many have their own privacy legislation. Agencies responsible for federally regulated sectors such as financial services, transportation and telecommunications often apply their own data requirements. Canada’s approach will also need to be compatible with the approaches taken by our major trading partners.

If our government gets this right, it will unlock the economic potential of the data-driven economy, strengthen productivity, and position Canada as a destination for investment, talent, and ideas. If we get it wrong, economic activity will shift to other jurisdictions and the living standards and well-being of Canadians will suffer.

What we heard

Regardless of the sector, Canadian companies are pursuing opportunities to use data and AI to solve key business problems and create new value. They are committed to doing so in a way that protects the rights, privacy and security of Canadians and their data. But they also report significant challenges, ranging from regulatory uncertainty and skills gaps to the cost of cybersecurity and data governance.

What we heard about the importance of data to Canadian business today is consistent with Statistics Canada estimates that Canadian organizations are investing up to $40 billion a year in data, databases, and data science. Eighty per cent of this investment comes from the private sector.

The companies that took part in our consultations told us they believe Canada has clear advantages it can leverage to support data-driven innovation. Our country is a global leader in AI research. Clusters in Montreal, Toronto, Edmonton and Vancouver helped drive a nearly five-fold increase in AI and machine learning job opportunities between 2015 and 2017, according to Deloitte.

It is critical that the private sector play a role in shaping Canada's data strategy. Every day, companies make decisions about which problems to solve with data, how to gather it and how to extract insights. They decide how much to spend on it. They have direct knowledge of fast-changing operational realities and the latest best practices. They also have a responsibility to contribute to the policy development process, working with government, the public and other stakeholders to ensure that data-driven innovation benefits all Canadians.

Everyone is in the data business

Nearly every company consulted for this study said that data, and the digital transformation that enables its collection and use, are major priorities for their business. They use data to foster deeper and richer relationships with customers, design better products and services, manage assets and risks, and improve operational efficiency. Examples:

Saving customers money: Customers expect financial institutions to respond quickly to their needs and help them save money. Banks and insurance companies are responding with new products and services. RBC's AI-driven virtual assistant NOMI provided more than 950,000 insights to customers since it launched, driving use of the bank's mobile app and helping users to save more. At Sun Life, a digital coach, Ella, provides clients with relevant and personalized advice, including health benefit account balances and retirement savings options. Ella emails clients with important reminders and can help them find the closest and most highly rated healthcare providers. In 2018, Ella helped 1.8 million clients save $400 million toward their retirement and obtain more than $375 million of increased insurance coverage. Intact Insurance offers reduced auto insurance premiums to drivers who use an app that tracks data on braking and acceleration, among other factors. The app can detect when the driver is using public transit or a taxi rather than his or her personal vehicle, thereby ensuring that only relevant data is captured.

Improving patient outcomes: Data-driven innovation is helping the healthcare system save time and money while helping patients. At Toronto's 650-bed Humber River Hospital, GE has developed a Command Centre for vulnerable patients that integrates predictive analytics, real-time information from multiple digital systems, and professional expertise. Clinical staff are alerted to potential changes in a patient's condition, allowing them to intervene earlier. The initiative has freed up beds and shortened emergency wait times, even as the numbers of patients served has grown.

Helping farmers enhance crop yields: Data-driven insights are revolutionizing every aspect of agriculture. Farmers Edge, a Manitoba-based software company, accumulates data from more than 100,000 fields a day. The company uses predictive modelling to optimize everything from crop choice in the spring to tractor speed throughout the planting, growing and harvesting cycle. Through a partnership with Winnipeg-based Richardson International, Farmers Edge markets its services to growers through 90 retail locations across Western Canada.

Making mining safer, cleaner and more efficient: Vancouver's Teck Resources collects data from sensors installed on mine equipment and uses AI to improve both operational efficiency, sustainability and safety. The company worked with MineSense, a Vancouver start-up, to develop "smart shovels" that detect ore grades and concentrations, which helps improve productivity and reduce waste. Teck has also partnered with Pythian, an Ottawa-based data specialist, to aggregate years of maintenance history for Teck's fleet of 300-tonne coal haulers and develop predictive algorithms that will save the company $1.5 million a year at one B.C. mine. Similar innovations are enabling workers to remotely control machinery in dangerous environments.

Improvements in forestry and fishing: Advances in connectivity and sensing technologies are helping companies manage natural resources more sustainably. Clearwater Seafoods uses LiDAR (Light Detection and Ranging) to create 3D maps of the ocean floor and now harvests scallops 60 per cent faster while dragging 70 per cent less seabed. This protects breeding grounds and helps stocks recover more quickly. On the other side of the country, Vancouver Island-based Mosaic Forestry uses LiDAR to map mountain forests and then applies machine learning to more accurately judge the height and diameter of trees, wood quality and other values. This allows the company to develop more accurate and sustainable forest management plans, preserving more of the forest resource. It is also much safer than manual inspections.

Building on time and on budget: PCL, an Edmonton-based diversified general contractor, created a software tool, PartsLab, that automates data flows between building design and construction teams. It reduces the time spent creating and managing documents from hours to minutes, limits discrepancies and improves workers safety. PCL is exporting the model, which now has nearly 3,000 users in 50 countries. For its part, EllisDon partnered with Bespoke Metrics to reduce supply-chain risk by standardizing and centralizing industry data. In addition to seed capital and preconstruction expertise, EllisDon provided Bespoke Metrics with 10 years of prequalification data that was used to optimize an analytics model that drives a suite of preconstruction tools ranging from subcontractor prequalification and performance ratings to tendering and bid submissions. The technology is now being used by more than 4,500 U.S. and Canadian subcontractors.

Improving legal services: Legal research is a major component of the cost of legal services. A Toronto-based AI lab owned by Thomson Reuters developed a specialized search engine that has dramatically reduced the time required to perform legal research, while improving accuracy. The development team used digitized texts and judicial opinions to train machine-learning algorithms that can dissect complex patterns within court decisions and precedents. Lawyers who use the technology can now dedicate more of their time to being effective advisors and strategists for their clients.

Challenges for Canadian business

As those examples illustrate, a growing number of Canadian companies are making strides in the data-driven economy. However, the competition is fierce and the transition is not easy. A 2018 report by McKinsey and the Business Council of Canada found that most large Canadian companies had yet to make the move from traditional data analytics to the predictive power of machine learning and other sophisticated forms of AI. Research by Deloitte, meanwhile, shows that even many early adopters of AI in Canada have investment plans that are less ambitious than those of their global peers.

The Canadian companies that participated in this consultation have encountered a range of hurdles in their efforts to use data effectively. They include challenges in earning consumer trust, cybersecurity, regulatory issues, an uneven playing field with newer digital competitors, insecure legal rights and a shortage of skills or data governance capacity. These hurdles make it harder for businesses to access and use data, making them less likely to invest in data-driven innovation.

Consumer trust: Overall, Canadian companies report high levels of trust with their customers. Consumer-facing businesses have typically made individual privacy a top corporate priority, with leadership often coming from the CEO. Trust is an essential precondition to the more personalized relationships they strive to build with their customers. Still, companies worry that their efforts to protect privacy could be undermined by high-profile data breaches and misuse by others, as well as by overly eager regulatory scrutiny. Consumers need to know that there are strict rules, and appropriate penalties for those who violate them.

Cybersecurity: The most frequently cited issue during our consultations was cybersecurity. It affects both B2C and B2B companies and the risks are increasing with the growth of IoT. Cyber-attackers can steal, destroy, or manipulate and falsify data used to control everything from medical devices, autonomous vehicles, and heavy machinery to entire energy grids. In the words of one executive, cybersecurity is the “foundation of a digital economy.” If companies and individuals aren’t confident that their suppliers or partners are operating in a safe manner, they will be reluctant to share data.

Regulatory compliance and uncertainty: Even the most well-intentioned data rules can hold back innovation, job creation, or undermine the protection of privacy if they are unduly difficult and costly to implement. PIPEDA is principles-based and technology-neutral, which is an advantage because it enables companies to determine the most effective and efficient means of meeting their obligations. But that also leaves more room for interpretation and can create uncertainty when companies are subject to both federal and provincial privacy legislation. One company reported that it dropped an otherwise promising data project because it could not get sufficient clarity around its privacy obligations. Differences in data regulation across the country can act as interprovincial trade barriers. International inconsistencies are similarly a barrier to growth, investment and competition.

Data localization: Canadian companies are concerned about growing efforts by governments around the world to restrict the flow of data across international borders. Some point to a now-rescinded proposal from Canada’s privacy commissioner that would have required organizations to seek additional consent from individuals for any transborder transfers of personal information to third-party processors. A typical large Canadian-headquartered company transfers personal information of customers, employees and suppliers to multiple service providers around the world daily. It does this to take advantage of secure cloud computing and storage, as well as to support basic business processes, such as human resources, legal and shipping. Companies are transparent about these activities and how they protect data internationally. But requiring them to obtain consent for every transfer would be impractical and in many cases impossible.

Level playing field: Many companies are concerned about the growing imbalance in access to, and control over, data. Large multinational digital platforms have amassed massive volumes of personal data and face relatively few restrictions on their use of that data. Unable to compete head-on with those platforms, Canadian companies often have little choice but to join their ecosystems. Certain regulatory policies can reinforce such imbalances. For example, Canada’s privacy law requires providers of paid services to seek separate consent to use personal data for marketing purposes. Companies such as social media platforms that provide free services are not required to obtain such consent.

Proprietary data: Businesses are often confused about their rights to use and treat as proprietary the data they collect. As one company put it, “Why invest in data if you can’t capture its benefits?” For example, the distinction between personal data on the one hand, and proprietary or derived business data on the other, is fuzzy. Do certain types of personal data become proprietary when they are derived, de-identified, anonymized and/or aggregated? Does data become proprietary when a company uses it in combination with other data to add value to a service?

Companies are also concerned about requests from government for access to data that is later shared with others. Similarly, some say it is difficult to assert or protect their data rights with partners or vendors. These often depend on contractual terms that are not well-tested in court, and the law is evolving.

Recommendations

The experts who participated in this consultation are convinced that, with the right policies and leadership, Canada can overcome many of the challenges that currently impede data-driven innovation. They believe that changes to the legal and regulatory framework and targeted investments in key sectors can create a future in which:

- Canadians have confidence that their data and rights are protected and secure;
- Global investors see Canada's data policies and regulatory framework as stable, clear and future-oriented;
- Businesses can access the data they need to deliver innovative products and services; and
- All Canadians benefit from data-driven innovation.

We asked companies to identify concrete actions that government and business could take to achieve these goals. The consultations yielded many ideas. This report puts forward 24 recommendations in three areas: protecting Canadians, supporting a competitive marketplace and building data infrastructure. In most cases there was a high level of agreement on the urgency and importance of the issue, as well as on the most appropriate solution. In a few cases, we were unable to reach a consensus given the wide variety of stakeholders. Some issues are addressed but only at a general level, and will therefore require further consideration by government and industry.

Protecting Canadians

Canada will not be able to develop a strong, data-driven economy without a foundation of trust, which in turn requires a policy framework that supports high levels of data protection. Canadian businesses are investing in privacy and cybersecurity because they see them as a competitive advantage. They understand the need to give clients, employees and suppliers the confidence that the data they share will be protected and used responsibly.

One company consulted for this study said Canada should embrace a model of "privacy-led innovation," which can achieve an "outcome that protects privacy and security without unrealistically burdening business or diminishing Canada's international competitiveness."

Most participants agreed that Canada's privacy framework is respected internationally. One company spoke of leveraging Canada's privacy brand to build partnerships with companies in Europe and the United States. PIPEDA, the federal privacy law that governs companies' collection, use and disclosure of personal information, came into effect in 2001 and was seen at the time as pioneering. Companies report high levels of compliance and agree that the technology-neutral, principles-based model has allowed PIPEDA to adapt to new technologies and developments.

Still, the world has changed a lot since PIPEDA was written. Personal data has become a much more significant part of the economy, leading to growing calls for Canada to reform its regime. High-profile data breaches, cyber-attacks and misuses of data are a growing concern for the public. The international landscape is evolving, too, as countries and regions move to implement new privacy frameworks, from the EU's GDPR and California's *Consumer Privacy Act* to proposed new U.S. federal legislation.

Canadian business leaders believe there is room to modernize and strengthen Canada's policy frameworks in ways that will help individuals and companies better protect their data from a range of potential harms – including accidental release, fraud and theft, unauthorized access and inappropriate use.

Our consultations identified several areas for improvement. Among them: potential amendments to PIPEDA dealing with consent and transparency, automated decision-making and algorithms, the right to erasure, and enforcement. In addition, the federal government can and should do more to support cybersecurity throughout the economy.

Make consent more meaningful

The requirement to obtain consent is a core tenet of all privacy legislation. It empowers individuals to choose when and with whom they share personal information. It provides organizations with the legal basis on which they can collect, use or share that information – facilitating a marketplace in which parties can opt to exchange value fairly.

Consent must remain a cornerstone of Canadian privacy law, but there are problems with Canada's current approach. PIPEDA's consent provisions require organizations to outline and communicate all potential uses of personal information. This can give rise to complex, lengthy and frequently amended privacy policies, often 4,000-5,000 words long. Few people have the time or expertise required to read and fully understand these policies. This contributes to "notice fatigue." Most people simply scroll down and click "agree," which suggests that their consent is not particularly well-informed or meaningful. By the same token, customers may not fully understand the implications of withholding consent. In some cases, failure to provide consent can deny companies the information they need to provide even basic services that the customer expects, such as product delivery and billing.

At times, it may not even be possible to obtain consent. The widespread adoption of data analytics and AI technology has given organizations the ability to use archived information in new ways, to deliver new services. In such instances it may be difficult or impossible to go back to the original source of the data and request permission for the new intended use. In other cases, data may be "observed" rather than willingly provided or volunteered. This might include records of a customer's interaction with an organization, or publicly available information such as court documents, public social media postings or data collected by smart city technologies such as road sensors. Consent requirements can also make it difficult to collect representative samples for statistical purposes, introducing potential data-quality issues.

The solution to these problems is to require consent when it is feasible to obtain, and when the intended use of the information would significantly affect individual privacy. Canadian legislation should require organizations to explain in simple, plain language how they intend to use the personal information they collect, with whom it will be shared, and the potential risks involved. The law should also give organizations the scope to develop user-friendly and easy-to-understand consent interfaces rather than highly legalistic formats. The law should support the use of "layered consent" or "permissioning," which would allow individuals to easily manage different levels of data-sharing based on their preferences. And the law should also continue to support the use of implied consent when information is less sensitive.

PIPEDA should also create legal grounds beyond consent that apply to the collection and use of personal information. Section 6 of the GDPR, for example, allows organizations to process personal information when doing so is necessary for the performance of a contract, compliance with another legal obligation, or to advance the vital interest of the data subject, public interest or legitimate business interests. In these cases, consent is not required. Canada should have a similar carve-out from consent for "legitimate interest" or "standard business practices."

Such changes would not erode personal privacy if the Privacy Commission were to issue guidance to ensure that potential risks are addressed. For example, processing based on "legitimate interest" or "standard business practices" could be conditional on an organization showing, upon reasonable request, that it has taken appropriate steps to minimize the privacy impact risk to individuals. This could include a formal risk assessment to ensure that the benefits outweigh potential impacts on an individual's rights, and that risk mitigation and other controls are in place. Such assessments would reinforce accountability and transparency, two key PIPEDA principles. Canada could also consider prohibiting certain uses of personal information, whether through PIPEDA or some other legislation.

Taken together, these reforms to consent models would limit the frequency of consent requests, make them more digestible and help Canadians make smarter decisions about their personal information.

Recommendations

Recommendation one: PIPEDA should be amended to require organizations to seek consent in a simple and clear manner, provided that such consent is feasible to obtain and the intended use of the information is of material significance to individuals. Specifically, PIPEDA should:

- require organizations to use plain-language explanations of the intended use of the personal information and any potential disclosure to third parties;
- encourage the use of “layered consent” or “permissioning,” to give individuals a greater degree of choice over what data is collected or used and for what purposes;
- continue to allow the use of implied consent when information is not sensitive, or the intended use is within the reasonable expectations of the individual.

Recommendation two: PIPEDA should provide legal grounds on which organizations can use personal information without consent, including when it is necessary for:

- the execution of a contract;
- to meet legal obligations;
- to protect an individual’s vital interests;
- to promote the public interest; or
- to support a legitimate interest or standard business practice.

When relying on alternatives to consent, PIPEDA should outline necessary additional conditions or protections, such as:

- enhanced transparency of data-management practices;
- clear senior accountability for adherence to those practices;
- demonstration of compliance with recognized data privacy codes or standards.

Recommendation three: Canadian law should prohibit certain uses of personal information and certain information-gathering practices. Examples might include:

- Seeking consent for the unlimited right to share personal information with third parties;
- Intentionally re-identifying information that has previously been de-identified, anonymized or aggregated;
- Requiring users to waive all personal information rights in order to access a product or service;
- Seeking consent from an individual under the age of 13.

Protect against bias and discrimination

Companies and governments are increasingly using algorithms to enable automated decision-making. In most cases, these applications improve the quality and accuracy of decisions. However, some algorithms can produce results that are undesirable or that amplify the biases of their creators. A widely reported example concerns an experimental machine-learning hiring tool at Amazon that decided male job applicants were preferable because it was based on submissions from the preceding 10 years, which disproportionately came from men.

Such issues are not new and have been the subject of human rights cases, notably in the insurance industry where age and other characteristics are customarily used to assess risk and determine premiums. Canadian courts have long held that certain differential treatment is permissible if it is “reasonable and bona fide.”

Nonetheless, some observers have proposed that organizations should be more open about how personal data is used in algorithms and automated decisions. In its consultations on PIPEDA reform, the federal government has suggested that the law could require organizations to disclose the use of, and factors involved in, such automated decision-making.

In our consultations, companies told us that they are willing to provide more information about their use of algorithms and automated decision-making, provided that the requirement to do so is limited. If the requirement is too broad, companies fear that they could be forced to disclose proprietary algorithms to competitors, which would reduce the incentive to invest in such software. Algorithms are also constantly changing, making it impossible to have a static disclosure.

A better approach would focus on developing and ensuring ethical practices, not just transparency, and holding organizations accountable for undesirable outcomes. For example, companies could guard against bias by incorporating diverse stakeholders in the development of new decision-making systems. The Montreal Declaration for Responsible Development of Artificial Intelligence hopes to guide companies that use AI systems to think about the moral implications of this increasingly powerful technology. More than 2,000 scientists and institutions have endorsed the Declaration since its publication in 2018. Canada's CIO Strategy Council also recently released guidelines for the ethical design and use of automated decision-making systems. Provincial human rights, employment and consumer protection laws should be the primary means by which complaints about bias are addressed.

Recommendations

Recommendation four: To help Canadians understand how their personal information may be used in automated decisions that affect them, PIPEDA should:

- require organizations to provide individuals with an overview of the factors involved in such decisions, the logic upon which decisions are based, and the potential impact on that individual;
- make it clear that it is not necessary for organizations to disclose information of a commercial or proprietary nature.

The right to be forgotten

Some newer examples of privacy legislation, including the GDPR and California's new law, contain a "right to be forgotten." This gives individuals the right, subject to certain limitations, to insist that organizations delete personal information about them that is out-of-date or potentially embarrassing.

PIPEDA already requires that organizations in Canada dispose of personal information when it is no longer needed. However, the federal government has suggested that the level of compliance with this rule is low. As a result, it is considering more specific rights for individuals to have their personal information deleted. It is also contemplating retention period limits and an obligation for organizations to track changes and deletions to maintain the integrity of the information.

The companies consulted for this study recognize and support the right of individuals to request that personal information be deleted. But there are implementation challenges. For example, unrestricted obligations to delete data may conflict with legal or regulatory obligations, as in the case of mandatory record-keeping to counter fraud or other criminal behaviour in the financial sector.

Companies are also concerned about the scope of such a legal obligation. It is one thing to erase the profile of a consumer who no longer wishes to participate a loyalty points program. It is quite another to remove that individual's anonymized purchasing history from broader datasets that are used to drive better business decisions. In addition, there are concerns that the right to be forgotten could be abused by individuals to restrict free speech and suppress information that is in the public interest – a matter that is currently being considered by the Canadian courts in a reference from the Privacy Commissioner.

Recommendations

Recommendation five: The government should reaffirm that Canadians have a limited right to request that organizations delete their personal information, subject to explicit exceptions. Specifically, PIPEDA should:

- define how and when an individual can request the deletion of personal information, and lay out reasonable response timelines;
- limit the scope of the right so as to exclude:
  - personal information that has been anonymized or de-identified, as well as derived data;
  - personal information used for journalistic purposes or academic, artistic or literary expression;
  - personal information that is being used under alternative grounds to consent (as outlined in Recommendation 2.)
- require organizations to inform individuals at the point of collection that they have a right to request deletion of their personal information, and explain how to do so;
- require organizations to make reasonable efforts to maintain the accuracy and integrity of personal information for as long as they hold it (i.e. throughout the chain of custody).

Strengthen enforcement and oversight

Compliance with PIPEDA is overseen by the Office of the Privacy Commissioner (OPC), which functions as an ombudsman – a neutral third party – in investigating and mediating complaints. The OPC negotiates voluntary compliance agreements and can refer cases to the courts or to the Attorney General of Canada for prosecution of specific offences. Since 2018, organizations have been required to report major data breaches to the OPC and can be fined if they fail to do so.

It is important to note that federal privacy laws do not function in isolation in holding companies to account for their privacy practices. Provincial privacy regulators are playing an increasingly active role, as is civil litigation. The Competition Bureau can also act against companies that misrepresent their privacy practices to customers.

Nonetheless, there is a perception that PIPEDA lacks the teeth of some other regulatory regimes, notably the GDPR. This view threatens to undermine confidence and trust in Canada's privacy laws, to the detriment of consumers and businesses. But the companies that participated in our consultations believe it is important to move carefully in strengthening Canada's enforcement and oversight model. They caution against adopting the overly prescriptive approach of the GDPR, which gives data authorities sweeping order-making powers and administrative discretion to issue fines worth up to four per cent of global revenues. Penalties on that scale, in the absence of established procedural safeguards, create tremendous uncertainty for business and can put a chill on data-driven innovation.

Canada should instead build on the successful and proven ombudsman model. This can be done by giving new tools to the OPC, such as limited order-making powers to assist with investigations. Federal law could also establish new prosecutable offences and financial penalties, responsibility for which should rest with the Attorney General and the courts. Fines should apply only to egregious cases of non-compliance, such as gross negligence or the intentional misuse of personal information. Companies should not be punished for data breaches that occur despite their best efforts.

Certainty about PIPEDA's provisions, and how companies can comply with them, is essential. As stated above, the fact that it is principles-based and technology-neutral has allowed PIPEDA to adapt to changes in business practices. But companies should also be permitted to take advantage of recognized industry codes, standards and certifications. The OPC and the courts should consider adherence to these as evidence of an organization's due diligence or as a mitigating factor in investigations.

The OPC could further reduce uncertainty by issuing binding individual guidance or pre-approvals at the request of companies. (This would be similar to the approach taken by the Canada Revenue Agency, which regularly issues "advance income tax rulings" and voluntary disclosure tools to improve compliance with the tax code.) To improve transparency, OPC should publish all its decisions in a timely manner, allowing other companies to learn from them and see how the law is being interpreted.

In summary, companies told us that they support expanded enforcement and oversight, but believe that it would be best served by the development of a shared culture and common understanding between the OPC and regulated companies. The OPC should prioritize private sector experience in its hiring and maintain regular engagement with industry experts.

Recommendations

Recommendation six: Strengthen Canada's existing enforcement model with new investigative tools, prosecutable offences and penalties for serious violations of PIPEDA, including by:

- providing the Office of the Privacy Commissioner with limited new powers to order organizations to cease activities that threaten imminent material harm to an individual, as well as to preserve records relevant to a case, subject to necessary procedural safeguards;
- extending the existing fine regime to other provisions of the law; and
- increasing the maximum fines available to the courts in cases of intentional or egregious violations of the law.

Recommendation seven: To reduce uncertainty and encourage the adoption of best practices in privacy protection, the government should:

- require the OPC, under the guidance of the Department of Innovation, Science and Economic Development, to maintain a list of recognized codes, standards and certifications;
- recognize adherence by an organization to a recognized code, standard or certification as evidence of its compliance with PIPEDA or as a mitigating factor in investigations and fine assessments.

Recommendation eight: The government should provide organizations subject to PIPEDA with voluntary compliance tools modeled on those of the CRA, including options to:

- seek a binding pre-approval or opinion from the OPC about a data use case;
- disclose unintentional misuses of data to the OPC and pursue remediation without fear of punitive measures.

Boost Canada's cyber-defences

Canadian companies consulted for this study overwhelmingly identified cybersecurity as a top policy priority and a prerequisite to higher levels of data protection. Cyber attacks threaten national security and public safety and are therefore the responsibility of government as well as the private sector.

But cybersecurity regulation has its limits. Requiring companies to use a common set of known practices can create systemic vulnerabilities. Holding organizations liable for cyber incidents that are beyond their control is unfair and counter-productive and does little to deter perpetrators. What is required is deeper collaboration between industry, law enforcement agencies and the intelligence community.

Accordingly, many companies welcome the new Canadian Centre for Cybersecurity, which provides industry with threat information and functions as a central contact point for Canada's security agencies. However, some companies raised concerns about the agency's capacity to respond to more frequent requests for assistance. Our consultations suggest that much more could be done to raise awareness of best practices, build cybersecurity skills, strengthen law enforcement and improve information-sharing.

Recommendations

Recommendation nine: The government should strengthen Canada's cyber defences and improve collaboration with the private sector by:

- investing more in cybersecurity awareness, education and measures to encourage the adoption of best practices by individuals and companies;
- devoting more resources to the investigation and prosecution of cybercrime, including a predictable funding model for the RCMP and the Canadian Security Establishment;
- introducing tougher penalties for cyber crime;
- allocating more funding for cybersecurity training and "white hat" hacking to test cyber-defences;
- supporting the expansion of the Canadian Cyber Threat Exchange, which enables cross-industry data-sharing and collaboration on cybersecurity initiatives.

Supporting a competitive marketplace

While security and privacy are paramount, Canada's policy framework also needs to encourage market players to share and exchange their data in ways that unlock value, drive innovation and contribute to economic growth. Markets work best when parties have clear rights to their property and are free to exchange them with other parties, with minimal barriers to entry and a regulatory environment that builds trust without being overly burdensome.

Today, many of these features are absent in the data economy. Data is not necessarily "owned" in the same sense that physical assets – or even other forms of intellectual property – are owned. Data is often locked in silos and therefore difficult to access and share. Increasingly, data is concentrated in the hands of a small number of dominant digital platforms. These platforms can use their gatekeeper power to direct consumers to their own sales channels, or to extract better terms from other market players. As mentioned previously, there are also growing barriers to the flow of data across domestic and international borders.

In response to these challenges, countries around the world are exploring new marketplace frameworks intended to give individuals and businesses more control over their data, promote competition and ensure the free flow of data. Many of these developments are in their infancy. Canada has an opportunity to help shape the future of data policy by creating a regulatory environment that unlocks the value of data for all Canadians.

Help consumers use their data

The push to create new market frameworks for data can be seen in the growing trend toward consumer data portability. Data portability is the right of an individual to access personal data held by an organization or to request that the organization transfer that data to a third party on his or her behalf. Examples include exporting a playlist from one music-streaming site to another, accessing data from an energy utility and entering it into a carbon-footprint calculator, or providing bank account history to a potential lender or aggregator that can advise on personal finances. Allowing users to move their data from one service to another promotes competition and gives new entrants access to data they otherwise would not have.

Governments are moving towards incorporating the right to portability in their legal and regulatory frameworks. The United Kingdom launched an open banking initiative in 2018. Australia has established a broader consumer data right, which will apply first to the banking sector and eventually to utilities and telecommunications providers. Both the GDPR and the California Consumer Privacy Act grant users a right to data portability and require that information be provided in a usable format that allows for easy transmittal. The Government of Canada recently held consultations on open banking and is considering whether to incorporate a portability right in PIPEDA.

Many of the Canadian companies consulted for this study see value in data portability. One called it “a foundational element of data-driven commerce.” Allowing users to transfer their data from one service to another promotes competition and enables new entrants to compete more easily for customers. It also eliminates unsafe practices such as “screen-scraping,” by which users willingly share login information and passwords with a third party so it can access their account.

On the other hand, many companies are concerned about the privacy and cyber risks, not to mention the significant costs of implementing full portability. Some point out that if they are required to share data with their competitors, it will become more difficult for them to generate a return from their data investments. That, in turn, could reduce the incentive to innovate.

For all of those reasons, data portability between organizations needs to be implemented carefully. Participating organizations should be accredited or contractually bound to ensure they have adequate cybersecurity and privacy practices in place. There should provisions to ensure that such practices do not create anti-competitive obstacles for new entrants. In addition, the right to portability should not extend to proprietary business data. Experience in other jurisdictions suggests these matters should be addressed on a sector-by-sector basis and can be either regulation-driven or market-led. In any case, industry should be closely involved throughout the process.

In short, any data portability right in PIPEDA should be narrowly defined. PIPEDA already gives individuals the right to access personal information held by an organization. The law could be amended to require that organizations make some of this information available to the individual in a digital format within a specified period. Companies will need appropriate time to invest in the necessary capacity.

Separately, the law needs to address data transfers between organizations. The GDPR grants individuals an unconditional right to request organization-to-organization transfers, but does not specify how this should be implemented. This has created confusion, in part because organizations are unsure how to comply while still meeting their obligation to protect information from unauthorized disclosure. It will be important for Canada to avoid similar confusion. It can do so by making it clear that the right to data portability exists only where both the transmitting and receiving organizations are part of a government-recognized data portability framework.

Recommendations

Recommendation 10: PIPEDA should include:

- a right for individuals to request and receive personal data from an organization in a digital format within a reasonable period;
- a right for individuals to request that an organization transfer personal data directly to a third party, provided both organizations are party to a sector-specific framework recognized by the government;
- a clear exclusion for proprietary business data as well as personal data that has been anonymized, de-identified, or derived.

Any sector-specific data portability framework should:

- be developed collaboratively with industry and relevant sector regulators or agencies;
- require that participating organizations are accredited or contractually bound;
- prescribe safe and secure means of data transmission;
- ensure adequate privacy and cybersecurity controls;
- ensure ongoing data transfers take place for a specified and renewable period of time;
- specify how organizations should authenticate informed consent of the individual;
- clearly apportion legal liability and accountability across the data transfer cycle;
- fairly distribute the costs of transfers and infrastructure;
- clearly define the scope of data subject to transfer requests, as well as exclusions.

Clarify business data rights

Just as many consumers are seeking more control over their data, many businesses are looking for greater clarity about their own data rights. Before they make significant investments in data-driven innovation, companies want to know that they will have secure access to, and control over, those assets.

As noted above, it is important to differentiate between proprietary business data and personal data. The protections that apply to personally identifiable information should not extend to anonymized or de-identified data, derived data or insights that businesses generate through subsequent aggregation and analysis. Governments can help clarify this in broad terms or more narrowly on a sector-by-sector basis. Recent EU guidance on the GDPR, for instance, outlines a number of specific examples of data deemed non-personal, such as data on travel that has been aggregated to hide a person's individual trips abroad, or anonymous data used in statistics or in sales reports.

Some of the companies consulted for this study want more clarity on their data rights in a business-to-business context. Intellectual property rights, such as trade secrets or copyright, are ill-suited to the increasingly dynamic and real-time streams of data that businesses are using in their operations. Data rights are more typically defined on a case-by-case basis through contractual terms. However, some companies, especially smaller ones, say the lack of negotiating experience and jurisprudence in this area can render them incapable of accessing valuable data, or locked into relationships with a single vendor.

Overall, there is a clear preference for the flexibility of contractual terms rather than overt regulation or legislation of commercial data ownership. However, Canada could improve transparency and reduce power asymmetries by establishing model contracts and provisions that businesses could voluntarily use when negotiating data-sharing agreements. It is worth noting that the EU and Japan are pursuing initiatives in this area.

Recommendations

Recommendation 11: The federal government should:

- collaborate with Canadian companies and the legal community to design general and sector-based contracts or clauses that businesses could use on a voluntary basis to protect and assert control over their non-personal data;
- seek to use such model contracts in its own contracting with the private sector.

Enforce competition

When a small number of companies attract a critical mass of users, data becomes a significant source of market power. Stronger privacy and data-portability regulations can help address the resulting asymmetries. In Canada, the Competition Bureau has been asked to examine the effectiveness of current policy tools, marketplace frameworks, and investigative and judicial processes in areas such as data accumulation, transparency and control. Still, traditional competition policy tools can be hard to apply in marketplaces characterized by platform business models and non-monetary exchanges of data for value.

Many of the companies consulted for this study agree that Canada's competition authorities should closely monitor anti-competitive uses of data and the rise of "winner-take-all" markets. A key goal should be to ensure that Canadian incumbents and start-ups can compete on a level playing field with multinational technology companies in both consumer-facing and industrial sectors.

They caution, however, against action that would undermine the incentive for companies to invest in data-driven innovation. The government needs to strike an appropriate balance between encouraging more open exchanges of data, and protecting expensive investments that firms make to gain a competitive advantage.

Recommendations

Recommendation 12: The federal government should ensure that the Competition Bureau has powers and capacity to address anti-competitive use of data. It can do this by:

- working with industry to develop a common understanding of the relevant conditions and metrics that should be used to evaluate the need for enforcement action;
- properly resourcing the Competition Bureau to conduct such research and analysis and collaborate with other jurisdictions on major international cases.

Support cross-border data flows

Aside from certain limited provincial rules and federal measures related to national security concerns, Canada's current policies generally favour cross-border data flows. Most companies consulted for this study support this approach, believing that any significant increase in barriers to such exchanges would make markets less competitive and innovative. Though cloud services do increasingly offer customized location services, Canada's national market is simply too small to support the development of a full suite of technologies and services. Countries that enforce data localization policies and similar impediments typically face higher IT costs and slower economic growth, according to a 2017 study by the Information Technology Innovation Foundation.

Restrictions on cross-border data flows can also affect public safety and security. Companies report that data localization rules can prevent them from taking advantage of cybersecurity solutions from international vendors. In the financial services sector, such restrictions make it more difficult to share information related to terrorism, fraud and money laundering.

PIPEDA currently permits companies to transfer personal information to third-party processors abroad, but holds them accountable for ensuring the same level of privacy protection as required under Canadian law. Even so, there will always be risks. Foreign law enforcement agencies may request access to Canadian data that is stored within their territories, just as Canadian law enforcement agencies may make similar requests for access to foreign data held in Canada. Organizations that transfer data abroad should be transparent with their customers and clients about such transfers, the steps they will take to protect their data, and the fact that they are subject to the laws of the country in which their data will be stored.

Many of the companies consulted for this study welcomed the inclusion of data-flow provisions in Canada's recent trade agreements, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Canada-U.S.-Mexico Agreement (CUSMA). These agreements prohibit countries from imposing data-localization requirements and restrictions on cross-border flows, while providing flexibility for governments to address national security and maintain high privacy standards.

Recommendations

Recommendation 13: Organizations should be required to inform individuals if there is a possibility that their personal information will be stored or processed outside Canada. They should also make it clear that data stored or processed in another country will be subject to the laws of that country.

Recommendation 14: Canada's future international trade agreements should include provisions against data localization and other barriers to cross-border data flows, modeled on those in CUSMA and CPTPP.

Align and harmonize regulations

Canadian companies support aligned or harmonized privacy and other data rules at the provincial, national and international level. Currently in Canada, there are dozens of sets of rules across jurisdictions and regulators. British Columbia, Alberta, and Quebec each have their own laws governing how business handles personal data. (The federal government considers these to be equivalent to PIPEDA.) Most provinces have specific laws that regulate the collection and use of personal data pertaining to healthcare, education, and employment. In addition, regulators in sectors such as financial services, telecommunications and transportation often have their own rules concerning data management and security. Definitions and obligations can vary, creating higher compliance costs and discouraging data innovation.

Canada already has too many internal trade barriers, and it is vital to avoid the creation of additional barriers for data. Aligning data rules should be a priority for the federal, provincial and territorial governments, just as it is in other important policy areas where there are shared responsibilities. It is worth noting that Ontario is currently reviewing its data policies at the same time as the federal government. This is an opportunity for alignment.

Alignment at the international level is equally important. The EU's goal in adopting the GDPR was to create one common, high-quality framework for privacy protections across the bloc, harmonizing national laws and eliminating barriers to cross-border data flows. Many countries are following its lead. From California to China, there is growing convergence on key elements of that model.

The European Commission currently recognizes 11 non-EU countries as offering a level of data protection high enough to permit data flows from the EU without further safeguards. The EU's so-called "adequacy list" is up for review in 2020. Canada may need to reorient some elements of its privacy laws to retain its position on the list. Adequacy, however, does not require equivalence, meaning that Canada is free to chart its own distinct course within limits.

Canada should exercise its influence within multilateral organizations such as the OECD to drive international alignment on key data governance issues. These forums help governments develop common approaches and templates. For example, the OECD's Guidelines on Privacy and Transborder Data Flows – first issued in 1980 and updated in 2013 – have shaped privacy laws in many countries, including Canada.

Canada's leadership in AI research represents an additional opportunity to influence ethical norms and policy development, as evidenced by the December 2018 launch of the Montreal Declaration for Responsible Development of Artificial Intelligence. In August 2019, the federal government joined France at a G-7 meeting to launch the Global Partnership on AI. The partnership is intended to bring together researchers, governments, civil society and industry to build consensus on the opportunities and challenges posed by AI, as well as appropriate policy responses.

Recommendations

Recommendation 15: The federal government should collaborate with the provinces and territories to align or harmonize data strategies and policies and create a national market for the free flow of data. Specifically, the federal government should:

- ensure that a national data strategy is a key agenda item at meetings of the federal, provincial and territorial governments;
- identify inconsistencies in provincial and federal privacy legislation and seek to resolve them through the Canada Free Trade Agreement's regulatory cooperation process;
- work with the provinces and territories to develop template agreements to facilitate the secure sharing of standardized health and education data.

Recommendation 16: In tandem with Canadian industry, promote the development of global policy norms for data governance, including through the Global Partnership on AI.

Building data infrastructure

A data-driven economy needs common data infrastructure, including codes, standards, and common mechanisms, practices, or institutions that enable organizations to securely and efficiently collect, share, and integrate data. The federal government can help develop this shared infrastructure through public investment, industry coordination and the adoption of enabling regulation, and by making its own data available to the private sector. Government also has an important role to play in supporting data and digital literacy.

Develop codes of conduct and industry standards

Voluntary codes of conduct and industry standards for data governance help companies bridge the gap between general regulatory obligations and specific data management practices. They also support common practices across organizations and sectors – enhancing trust, interoperability and data-sharing opportunities. As noted above, PIPEDA should be flexible enough to allow companies to meet their regulatory obligations through adherence to recognized codes of conduct or standards.

While many codes and standards are currently in use across Canada today, the landscape is fragmented and incomplete. The Canadian Marketing Association, for instance, has its own Code of Ethics and Standards of Practice for digital advertising. Another example, Privacy by Design, is a standard that allows companies to certify that personal data is automatically protected in a given IT system or application; no action is required on the part of a user to protect his or her privacy because it is built into the system by default. Originally developed at Ryerson University, Privacy by Design is now the basis of a global standard being developed at the International Standards Organization.

Several Canadian industry and government bodies are developing new standards to address emerging data governance issues. Canada's CIO Strategy Council recently published a first-of-its-kind standard for "ethical design and use of automated decisions systems." One of the Canadian companies that participated in our consultations plans to apply this new standard throughout its global operations.

Digital identity is another area of focus. If individuals could quickly and securely authenticate their identity and other personal information, it would enhance cybersecurity, privacy and consumer value. The Digital ID & Authentication Council of Canada believes widespread adoption of digital identification could save consumers $6.1 billion a year. The council helped support the recent launch of Verified.Me, a digital identity network built by SecureKey with the involvement of major Canadian financial institutions.

Despite the move towards standardization, many Canadian companies continue to rely primarily on internally developed frameworks to govern their data and meet regulatory obligations. Canada needs a comprehensive strategy to bring these developments together and determine where industry needs are greatest. That is the mission of the new Canadian Data Governance Standardization Collaborative, a multi-stakeholder forum launched by the Standards Council of Canada. It plans to assess the Canadian and international landscape, identify gaps and produce a roadmap in mid-2020.

Many of the Canadian companies consulted for this study believe they have an obligation to support and participate in such exercises. More than a dozen of them have representatives on the collaborative's working groups. Many other countries provide funding to organizations that participate in standards-development initiatives. Canada should consider doing the same, particularly for start-ups and smaller companies that may not be able to afford the investment.

Standardization holds great potential over the medium and long term. In the meantime, several companies felt that they and the SMEs in their supply chains would benefit from general guidance outlining best practices for private sector data-sharing. Singapore's Infocomm Media Development Authority and Personal Data Protection Commission recently released a Trusted Data Sharing Framework that could serve as a model.

Recommendations

Recommendation 17: The federal government should support the efforts of industry to develop codes of conduct and standards for data governance, including by:

- ensuring adequate industry representation in the recently launched Canadian Data Governance Standardization Collaborative;
- seeking advice from the collaborative on the use of voluntary codes and standards to support compliance with federal regulatory regimes;
- bearing some of the cost of business participation in standards development, in particular for start-ups and SMEs.

Recommendation 18: The federal government should work with data governance specialists from a wide range of industries to develop and disseminate a practical toolkit to advise companies on data-sharing best practices.

Help sectors share data

In addition to general codes and standards, Canada needs to invest in more targeted data-sharing infrastructure. Many of the companies consulted for this study see a need to work together to find ways of sharing or pooling specific types of data, in part to counter the growing competitive threat posed by large, global firms with significant data advantages.

As with data portability for consumers, there are significant challenges associated with data-sharing among businesses. It requires common formats for structuring and communicating data, privacy and security controls, liability frameworks and a common understanding of what sorts of data can or should be shared rather than being treated as proprietary. Much of the infrastructure to support data-sharing must be built from scratch. And it often requires companies to make significant internal investments in data management systems.

One large construction company that took part in our consultations said that while better data-sharing could make its industry more competitive, supply chains are fragmented and filled with small players that lack proper data governance for even the most basic business processes and functions. As a result, the company has looked at joining U.S. consortiums that are further ahead in dealing with health and safety data.

Government funding and leadership can help to address the uncertainty, coordination challenges and potential conflicts involved in building such sectoral frameworks. Close collaboration with industry is essential to ensure that such frameworks address clear use cases and are technically feasible.

Canada should also explore the potential of "data trusts" to help individuals and organizations share sensitive data for particular purposes. Data trusts are essentially legally accountable governance structures that can oversee, maintain and manage the use and sharing of data. Governments and international organizations such as the OECD and the G20 have focused on the potential to use data trusts to promote data sharing and "responsible" innovation. The federal government's discussion paper on PIPEDA reform notes that data trusts could be used to alleviate the burden of consensual exhaustion and privacy self-management for transactions involving de-identified data. So-called "civic data trusts" have been proposed as a means of protecting the public interest in data governance decision-making processes. These are essentially contracts that give a group of trustees authority to manage the collection and use of data based on the trust's founding principles.

The concept of data trusts is still relatively new. Before they can be deployed at scale, core features of trusts – including the nature and scope of fiduciary obligations, as well as governance structures and technical architectures – will need to achieve a high level of standardization. It remains to be seen whether data trusts can deliver value beyond what can already be done securely through existing approaches. Business and government should work together to explore the potential of data trusts and the role government might play in establishing an appropriate regulatory framework for them. However, several companies that took part in our consultations said that participation in such initiatives should be voluntary; private organizations and individuals should not be required to pool their data.

Recommendations

Recommendation 19: The federal government should support efforts to develop sector-based frameworks that help companies pool and share data for specific purposes. This could include:

- public investment in several priority data-sharing or data-pooling initiatives with resources from existing programs such as the Strategic Innovation Fund or the Innovation Superclusters Initiative;
- providing access to relevant government datasets and the expertise of agencies such as Statistics Canada;
- maintaining an index of available application programming interfaces and data-sharing standards.

Recommendation 20: The federal government should work with industry to assess the business case for data trusts in sectors such as healthcare and urban transportation, as well as the need for a dedicated regulatory regime or governance template.

Leverage public sector data

The federal, provincial and territorial governments are stewards of enormous amounts of data. Governments need this data to develop good public policy, regulate effectively and deliver public services – including statistics on which the private sector relies to make business decisions.

In recent years Canada has taken steps to make its data more available, accessible and relevant to the problems that companies are trying to solve. The federal government's Open Data Portal now provides digital access to more than 80,000 datasets. But there is still much more work to do. Many of the companies consulted for this project do not even think of approaching governments for data partnerships. Those that do speak of frequent missed opportunities. For example, if the federal government gave researchers in the private sector access to high-resolution satellite photos, companies could train machine-learning algorithms that would help overcome transportation bottlenecks or improve Canada's response to climate change.

Governments should work with industry not only to determine what information can be made public, but also whether there is a need to collect it in the first place. Although federal laws give Statistics Canada and other agencies powers to compel data from individuals and companies, it is important to ensure privacy and confidentiality.

Finding the right balance can be difficult, as demonstrated by the 2018 controversy over Statistics Canada's attempt to launch a pilot project to gather the personal banking information of 500,000 Canadian households. Although the OPC's report into the matter found no fault, some in the private sector felt the request conflicted with the banks' privacy obligations to their clients. Statistics Canada has since adopted a "necessity and proportionality framework" that assesses the need for collection against other factors, such as the sensitivity of the data and whether there are other ways of collecting it.

As the government reviews the *Privacy Act* and the *Statistics Act*, it should further evaluate the grounds on which – and the processes through which – it collects and shares data. The goal should be to make high-value data readily available whenever possible, while protecting the data rights of individuals and businesses. It may want to consider specific carve-outs for data that is used for statistical and research purposes.

Canada should also consider what other jurisdictions are doing in this area. Australia's government, for example, has proposed new legislation to streamline the way public data is shared and released within government and with trusted users. A 2018 discussion paper said the objective was to "provide efficient, scalable and risk-based trusted data access to datasets that have substantial and community-wide benefits for research, innovation and policy." For its part, Saskatchewan recently adopted a law that promotes co-operation among government agencies when it comes to information sharing. The law allows government bodies to enter into data-matching agreements to participate in projects that make use of personal information, so long as they continue to protect individual privacy rights.

Recommendations

Recommendation 21: The federal government should provide the private sector and other organizations with greater access to high-value government datasets and data environments. This includes:

- developing a process for businesses to work with the federal government to identify and prioritize datasets or data environments on a project-by-project basis;
- establishing a framework for risk-based authorizations and trusted end-users in the case of sensitive data;
- ensuring that relevant business support programs, such as the Industrial Research Assistance Program, are identifying opportunities for their clients to leverage public sector data.

Recommendation 22: The government should work with industry to clarify the exceptional circumstances and rigorous processes under which government entities can compel organizations to provide personal or confidential business information.

Support data literacy

Data literacy is an essential part of a data-driven economy. To realize our country's potential in the data economy, Canadians will need to become digital citizens, with higher levels of awareness and understanding of how data affects their lives and work. They must be able to recognize the value of their data and make informed decisions about what they want to do with it.

Past efforts by government to enhance financial literacy offer examples that could be emulated and adapted to improve digital literacy. At the same time, governments should pay special attention to the digital literacy of smaller companies, which often have limited capacity to collect, manage and extract value from data. For many SMEs, privacy regulations represent a serious compliance burden.

The rapid adoption of data-driven technologies is also exerting increased pressure on government. Canada's federal government needs to build data governance capacity across departments and agencies. Other jurisdictions have addressed this need by establishing high-profile offices that can conduct research and provide guidance across government. The U.K. government created an independent advisory body, the Centre for Data Ethics and Innovation, to connect policymakers, industry, civil society, and the public. Israel's Ministry of Foreign Affairs has established a Data Diplomacy R&D Unit, which is pioneering an algorithmic approach to the practice of diplomacy. The United Arab Emirates recently appointed a Minister of Artificial Intelligence. Prime Minister Trudeau's decision in 2018 to appoint a Minister of Digital Government is an important step toward improving data literacy and governance capacity at the federal level.

Recommendations

Recommendation 23: The federal and provincial governments should develop a coordinated strategy aimed at fostering "digital citizens" through Canada's primary, secondary and post-secondary education systems, as well as through skills training programs.

Recommendation 24: The Government of Canada should provide informational support and resources for all Canadian businesses – including SMEs and start-ups – to improve their digital literacy. The goal should be to ensure that businesses not only comply with a modernized data governance regime, but also continue to innovate and thrive. The Business Development Bank of Canada and Export Development Canada may be best positioned to deliver this support, given their established networks of SME relationships.

Conclusion

Canadian business leaders across all sectors recognize the potential of the data-driven economy. They believe government and business need to act quickly to seize the opportunities, gain a strong competitive advantage, and ensure that Canada is an attractive destination for global investment, talent, and ideas.

At the same time, they recognize that the social and economic potential of data can only be realized if all participants believe that their interests are being protected and promoted. Individuals need to know that their data and personal information are safeguarded. When they choose to share their data, they need to know that they are receiving appropriate value in return. Businesses, for their part, need to be able to access and use data to compete and innovate on a global stage. Governments similarly need access to data so they can help citizens and deliver vital public services while protecting and promoting Canada's interests in the global economy.

Based on conversations with dozens of industry leaders and experts, this study found consensus on many concrete policy recommendations. They address key challenges such as privacy, cybersecurity, cross-border data flows, competition policy and data infrastructure.

All Canadians and all stakeholders have roles to play in ensuring that Canada makes the most of this economic opportunity. There is much work ahead, but if policymakers move quickly and make the right decisions, Canada can and will realize a future that unlocks the value of data for the good of all, while respecting the rights of all citizens.

Appendix

Advisory panel

Hon. James Moore (Chair)
Paul Ballew, SVP Global Chief Data and Analytics Officer, Loblaw Companies Limited
Chantal Bernier, Counsel, Lead, Privacy & Cybersecurity, Dentons
Kevin Dougherty, EVP, Innovation and Partnerships, Sun Life Financial Canada
Charles Eagan, Chief Technology Officer, Blackberry
Catherine Luelo, Senior Vice President & Chief Information Officer, Air Canada
Ben Harrison, Partner, Portag3
Rosemarie Lipman, Chief Information Officer and Senior Vice President, Enterprise Intelligence, EllisDon
Robert Malcolmson, Senior Vice-President, Regulatory Affairs and Government Relations, BCE Inc.
Anne Martel, Co-Founder and SVP Operations, Element AI
John Pecman, Senior Business Advisor, Fasken
Holly Shonaman, Chief Privacy Officer, RBC

Companies consulted*

Air Canada
AGF Management Limited
Bell Canada
Blackberry
Bruce Power
Cadillac Fairview Corporation Limited
Canada Life
Clearwater Seafoods
Cenovus Energy
D2L
Deloitte
DuPont Canada
Element AI
EllisDon
Enbridge
GE Canada
HP Canada
IBM Canada
Insurance Bureau of Canada
Intact Financial Corp.
KPMG LLP
Loblaw Companies Limited
Manulife Financial Corp.
Microsoft Canada
Morneau Shepell Ltd.
Mosaic Forestry
National Bank of Canada
PCL Constructors Ltd.
Pelmorex
Portag3
Power Corporation
Richardson International
Royal Bank of Canada
Scotia Bank
Sidewalk Labs
Siemens Canada Limited
Sun Life Financial
TD Bank Group
Telus
Thomson Reuters
TC Energy
Teck Resources Limited

**The opinions in this paper represent those of the Business Council of Canada and do not necessarily represent the views or positions of the consulted organisations above.*

Business Council
of Canada