ITAC ACTI
INFORMATION TECHNOLOGY
ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE
DE LA TECHNOLOGIE DE L'INFORMATION

LEVERAGING DIVERSITY, TECHNOLOGY & TALENT
Delivering a Secure Digital Society for Canadians

Developing a Data-Driven Digital Economy in Canada

JULY 2018

EXECUTIVE SUMMARY

Everywhere we look—regardless of organization, sector or industry—data is being increasingly leveraged to deliver better, more efficient solutions and services to citizens and customers.

And now as we enter a "digital renaissance" where everyone and everything is interconnected, data is becoming ever more important to how we solve life's most complex problems.

But despite the many economic and life-saving opportunities that leveraging high-quality data presents to businesses and individual Canadians, our country is not yet taking full advantage of all that data has to offer.

There are many reasons for this slow upswing. But perhaps the greatest obstacle—from a technological, sociological and psychological perspective—is the overarching concern for data privacy and sovereignty.

Unfortunately, these concerns continue to limit industry, academia and the public sector's ability to share and exchange data in real-time. And that, ultimately, means that these organizations are not innovating nor developing the products and solutions that are most needed today (not to mention, in the future).

The good news is that Canada can indeed create a successful framework for data governance that spurs economic growth, while also addressing Canadians' concerns regarding privacy and security measures.

The Information Technology Association of Canada (ITAC) strongly believes that Canada's government—in collaboration with the ICT industry and all sectors—must take an immediate and coordinated approach to data governance; and that such an approach must ensure privacy and security, while also unlocking data for economic prosperity.

This can be achieved by developing a strategy that:

- **Provides a long-term vision and enables a modern approach to data governance with clear guidance;**
- **Maximizes the value of data for organizations and recognizes that data is both a proprietary and a shared asset;**
- **Identifies priority areas for development and unlocking data to meet current and future needs of business, government, and civil society, and that supports innovation;**
- **Recognizes that Canada competes in a global digital marketplace and the data strategy can be leveraged to attract investment and allow Canadian firms to compete internationally;**
- **Ensures Canadians benefit from IP developed in Canada;**
- **Understands and balances privacy, consumer trust and the security needs of Canadians;**
- **Provides straightforward direction on transparency and accountability for organization that own, develop, collect, use and share data;**
- **Trains the next generation of Canadians supplying talent to meet data economy demands;**
- **Leverages our diversity and globally representative population to provide a test bed for data analytics;**
- **Understands that success requires partnerships and supports projects that integrates data from multiple sources; and**
- **Leverages the Federal Governments role as a convener to break down jurisdictional silos and foster collaboration.**

ITAC also recommends that the following 10 factors be considered in developing a national data-driven digital strategy:

1. **Artificial Intelligence (AI):** Ensuring the availability of high-quality to achieve the promise of AI, while also ensuring transparency and furthering controls of technology.
2. **5G networks:** Allowing adequate governmental funding for and incentivizing the roll-out of 5G technology, the backbone of the data economy.
3. **Trans-border data flows:** Unlocking data's economic potential to support and grow trade by facilitating the flow of data internationally.
4. **Quantum computing:** Understanding how "supercomputers" will play a role in a data-driven digital economy.
5. **Shifting from open data to integrated data sharing:** Progressing from open and available, to integration, meeting the needs of academia and industry with the objective of spurring innovation.
6. **Digital identities:** Enabling businesses and consumers to improve interactions through a secure and controlled digital identity management framework.
7. **Data ownership:** Develop simple and clear guidelines for governance, data generation processes, usage and sharing.
8. **Data security and privacy:** Encouraging the use of technologies (encryption, blockchain, etc.) to protect Canadians' data.
9. **Data protectionism:** Limit data protectionism policies and encourage a consistent approach nationally and internationally.
10. **Data residency and sovereignty:** Understanding that location of data does not guarantee security or limit access by foreign governments, and identifying better alternatives.

At the time of publication, no other country worldwide has a comprehensive framework or strategy for dealing with data governance. This therefore presents a unique opportunity to the Canadian government to become a global leader on this very issue.

Indeed, by creating national frameworks that clearly communicate how Canadians collect, use, disclose, and share data actively, there is no limit to what our country can ultimately achieve.

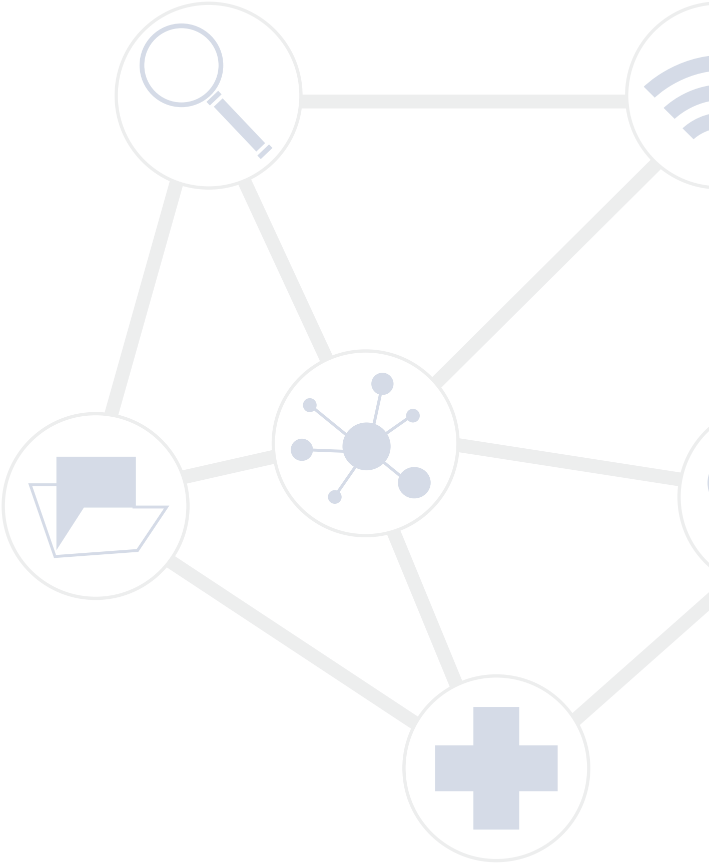


TABLE OF CONTENTS

Developing a Data-Driven Digital Economy in Canada

INTRODUCTION

Data. We are creating more of it each year than in all human history—and it is now considered to be the leading global commodity.

But what *is* data—and where is it taking us?

Simply put, data is a resource that can cross borders in unprecedented speed and fluidity:

- Enabling industries to capture and leverage process efficiencies increasing competitiveness and decreasing costs; and
- Leading to even greater technological and human advances than we have ever seen or experiences.

But what *is* data—and where is it taking us?

Indeed, data analytics—the discovery, interpretation and communication of meaningful patterns in data—are helping us address a multitude of market and societal inefficiencies to improve our mobility, health, environment, and quality of life.

By making the data exposed (in a manner controlled by the government), the foundation for the creation of new digital services by private industry and non-profit organizations is possible. According to IDC, a centralized digital platform is a new way of designing, building, integrating, and running IT that accelerates digital innovation at the scale and pace. A new enterprise IT architecture enabling the rapid creation of externally facing digital services, and experiences, while aggressively modernizing the internal legacy and core environments in parallel.

A defining element of the digital platform is that it is "driven by the data" with an ever-expanding variety of data pipelines connected in from outside the organization and that data (along with the government's own data) fueling the artificial intelligence-driven models and code that form the basis of the understanding of the digital citizen/consumer experience and their interactions with services.

Additionally, the importance and incentives of data in the business world cannot be overstated. Analytics are driving businesses by showing them how customers think, what they want, and how the market views products and brands. Essentially, those who know customers better, serve customers better—resulting in increased loyalty, heightened customer service, and knowledge of potential customers (often better than they may know themselves). Now and in the coming years, using a data-analytics approach will be a cornerstone of how all businesses operate.

Put more simply, over the coming decade, data will:

- Be the resource that defines Canada's collective economic opportunity; and
- Enable companies to disrupt traditional industries in a way that modern economies have never seen.

It is clear that with data, information is power; and the right data in the right hands can unlock solutions to make the world a better place.

However, the Canadian Information Communications and Technology (ICT) industry is rapidly outpacing government policies. Many of these policies are outdated and based on principles not for a digital but a *physical* or industrial age environment. Meanwhile, recent data breaches and use of citizens' data is also causing concern for individuals and businesses alike.

The question then is: given how much data can offer Canada and Canadians, **what can Canada do to position our country as a data-driven economy?**

The Information Technology Association of Canada (ITAC) strongly believes that Canada's government—in collaboration with the ICT industry and all sectors—must take an immediate and coordinated approach to data governance; and that such an approach must ensure privacy and security, while also unlocking data for economic prosperity.

OPPORTUNITIES FOR A DATA-DRIVEN DIGITAL ECONOMY

The Role of the Canadian Government

While some organizations have become quite sophisticated in how they leverage data, governments across Canada have been slow to leverage data-sharing to better serve Canadians—mired down by outdated policies and regulatory frameworks that were developed prior to the advent of the Internet.

Fortunately, governments are finally, albeit slowly, turning their attention to the issue. Federal investments in artificial intelligence (AI), quantum computing and fifth generation (5G) are good examples of planning ahead for a data-driven digital economy.

Governments are realizing that the movement of data across borders can generate significant economic and societal gains. These easy data transfers are an essential component of creating worldwide benefits, allowing companies and researchers to access expertise in all corners of the world to leverage their global experience and limit duplication of effort. Moreover, strengthening industries thriving on data helps reach shared goals of improving talent retention and building deeper public-private partnerships.

However, recent data breaches and misuse of citizens' data is causing significant concern.

Ultimately, a balanced approach is needed: one that addresses concerns about security and privacy, while also enabling businesses to leverage data in their control for value-generation purposes.

However, to be successful, there must be coordination between all levels of government, as well as industry, to unlock the data to allow for the development of new initiatives and innovations that support new market entrants—so both data producers and users can benefit. The federal government must lead a national dialogue that breaks down domestic barriers to data sharing between governments, academia and the private sector.

In this coordination of all levels of governments, best practices should be identified and adopted.

A balanced approach to data governance can be achieved without necessarily restricting and storing data behind jurisdictional borders (municipal, provincial or national), by:

- Creating a guiding framework for the usage, sharing and publication of data from public sector and industry alike; and
- Placing privacy and anonymization as a top priority— building the public trust needed to continue to evolve and strengthen this industry.

Building a Value and Intellectual Property Framework

The availability of high-quality data from governments and industry (and hence, a national data governance strategy) is one part of the equation.

However, having a value framework—where there is a financial incentive for industry to leverage, share and grant access to data—must also be considered.

The nature and extent of data is a significant asset to industry players, helping them generate new revenue streams (e.g., through building new products and solutions) and differentiate Canadian industry from global competitors. This will be true of many large organizations.

Together, both frameworks will contribute to a more comprehensive and sustainable national data strategy.

However, it is important to recognize that organizations will be reluctant to share information, hindering access to data across the country. Therefore, it will be extremely important to build a clear:

- **Value framework** that provides a financial incentive for organizations to share information—while also protecting the value of their assets; and an
- **Intellectual property (IP) framework** that focuses on the desirability of open data (i.e., market need), as well as the technical feasibility of data (e.g., privacy, security, delivery).

Releasing Data from the Internet of Things, Smart Cities, and Automated Vehicles

Digital transformation is making extremely positive changes to the way we work and live—particularly as citizens are increasingly connected to devices that are interconnected.

This is known as the Internet of Things (IoT): a network of devices, sensors, infrastructure, and connected and automated vehicles—essentially an ecosystem, driven by the data collected from these devices, in which solutions, applications and services can be developed.

In fact, the IoT is so prevalent that is it predicted to increase from 6.5 billion interconnected devices to more than 21 billion in the coming years.

IoT devices are being deployed in all business sectors: from health (including implantable devices like pacemakers, wearable devices like FitBits, and remote monitoring devices like tele-homecare) and education, to agriculture, mining and oil and gas, to transportation.

SMART CITIES

Meanwhile, the IoT is spurring the development of Smart Cities, which will lead to a massive increase in data—with data analysis facilitating new applications and efficiencies.

While there is no single definition for what makes a "smart city," the term generally applies to cities that leverage connected technologies to collect, analyze and act on data in ways that increase efficiencies and improve outcomes for citizens, visitors or businesses.

The basic idea of smart cities is not new. However, it is the possibility of technology to dramatically scale the amount of data collected—and to improve accuracy of insights gleaned from that data—that creates revolutionary opportunities.

Organizations see the benefits when they can overcome challenges and implement an IoT solution that harnesses massive amounts of data.

Over the last half century, two trends have re-shaped Canada's development—highlighting the incredible opportunities that Smart Cities present for Canada:

- First, there has been an accelerated move of Canadians to big cities. Just over 80 percent of Canada's population lives in urban areas, and roughly two-thirds of Canadians live in a census metropolitan area. With this influx of people into urban environments, dated infrastructure and municipal governance structures have found it difficult to accommodate this new populous.
- The second trend has been the expansion of connected technologies into virtually every area of our lives. We now use connected devices to work, shop, date; stay connected with colleagues, family and friends; and engage in our communities. While technology has made it easier than ever for individuals to connect globally, the data being collected through these media have also created incredible opportunities to build deeper knowledge and engagement.

Coordinating federal, provincial and municipal projects and investments in smart cities should take a long-term view of value on taxpayer investments. Indeed, investments in a "smart infrastructure"—that is, assets that can collect, communicate and potentially act on data—can represent better long-term investments for taxpayers. The data generated can inform things like maintenance schedules for public infrastructure and can—if combined with other data sets—support a plethora of additional policy or public benefit purposes.

All infrastructure decisions need to be made based on the specific circumstances of the project. That said, to promote innovation and future-proof tax payer investments, governments should at very least require funding applicants to consider opportunities to embed "smart technologies" into new infrastructure projects.

Leveraging Existing Data for Innovation

Data-driven digital transformation is playing out across all sectors: from oil and gas, to retail, to agriculture, and even professional sports and entertainment. For example:

- Data from intersections are being analyzed to better sequence the lights to improve traffic flow and decrease auto collisions, creating safer driving conditions.
- Bluetooth beacons set up in retail outlets can help track smartphones throughout the store, and thus record path-to-purchase data that can later be used to enhance store layouts and customer experience. IoT tech is not just about transmitting special offers and other information when we couple it with GPS tracking: it can also sense if a customer is within a certain radius of any store in the chain. Take it a step further, and retail centres can push information containing offers tailored to a customer's previous buying habits when they are within walking distance of the store.
- Data is being collected and used for our home management. It is not just about how Google Home or Alexa can respond to voice commands—they can also manage enabled devices in the home, control the thermostat to lower usage during peak hours (saving energy resources), control and give access to security cameras, and much more.
- In agriculture, Internet-connected sensors now in development can log data about the causes behind bees' worldwide disappearances, and farmers are using sensors to monitor water levels in crops.

However, leveraging data for impact isn't as simple as flipping a switch.

Weighed down by legacy technologies, outdated processes, regulatory burden and cultural obstacles, many organizations struggle to turn data into effective business outcomes.

It is difficult, if not completely unfeasible, to make business decisions based on incomplete or stale data. A lack of structured data will make it impracticable to run artificial intelligence (AI) and analytics to pursue more active outcomes.

The same can be said if data is separated into silos and hosted on multiple systems or applications. These foundational gaps leave businesses at a disadvantage when they try to extract insights from a virtually endless supply of potentially valuable information.

By treating data as a strategic asset—and leveraging trusted, accessible and timely data—businesses have an opportunity to better position themselves competitively. Organizations can help separate business units as well as customers and members within their supply chain to identify new opportunities to grow business, deliver superior customer experiences, and improve operational efficiency.

Just as data touches every line of business, every department, process and discipline, data can be leveraged to make significant bottom line impacts—across any project.

The Opportunity to Transform Health

Since Canadian health care is based on a single-payer system—and our country has a vast geography with a statistically meaningful population size—the opportunity to advance health care and health efficiency is huge and potentially unique in the world.

Subsequently, leveraging health and pharma data and combining data sets could lead to better health outcomes for Canadians via regional, provincial and federal collaboration.

Governments have been struggling to use patient data collected over decades to better address health issues facing Canadians. Indeed, there is a clear need for governments and regional health services to collaborate more across agencies and provincial borders to create better policies for better health for all residents.

Information sharing across the healthcare ecosystem relies on interoperability between disparate information and communications technology (ICT) solutions (e.g., lab, pharma, acute care and primary care systems etc.). In 2017, ITAC Health released a position paper, on this important topic, ITAC Health ISC Position on Canadian Healthcare Interoperability Standards.

In fact, improvements in health data liquidity—that is, the ability of patient data to move through the healthcare system securely and effectively—will benefit of Canadians in three ways:

- Better health-data sharing improves continuity of care, over time, and across different care-delivery sites. Evidence shows that improved care continuity directly impacts and improves individual patient outcomes.
- Individual patient data can be de-identified and used to drive population-level analytics. Machine-learning algorithms can run virtual randomized controlled trials on these big data to identify "positive outliers." From these, improved care pathways and novel new treatment practices can be mainstreamed to create what the US National Institute of Health refers to as the Learning Health System.
- On both an individual and population basis, better health is directly related to better economic performance. Although the goal of our healthcare system is to improve Canadians' health and wellbeing, success in this contributes to our overall GDP.

CONSIDERATIONS FOR A NATIONAL DATA-DRIVEN ECONOMY STRATEGY

The following pages include a list of factors for government to consider in its effort to create a national data-driven economy strategy, as well as a value framework and IP framework.

Consideration #1: Data Ownership

The issue of data ownership is an important one, as it encapsulates all types of data and metadata that are created, managed or used within organizations.

Ownership denotes a certain level of responsibility. It requires regulatory compliance when collecting personally identifiable information. It also requires compliance regarding things like time stamps and data accuracy. As such, owners can be held liable when questions arise about the data or its meaning.

The responsibility of "ownership" becomes increasingly complex when combining various types of data from internal as well as external sources; and dealing with social, structured and unstructured data. Moreover, depending on jurisdictional location of a business and its data centers, different data ownership rules may apply in different situations (e.g., how it is gathered, transformed, analyzed, interpreted, shared and moved).

As such, defining who owns and is responsible for the security and custodianship of an organization's data in different situations requires a certain level of vigour—as does determining the handling of personal or medical information; government, proprietary or top-secret data; employee records; financial records; or data concerning any regulated industry or industrial process.

UNDERSTANDING "DATA ORIGINS"

Anyone tasked with managing data or other resources where data are gathered, processed, and analyzed, may need to address ownership-related questions occurring anywhere along the "data value chain."

Here are two examples where an understanding of data origins will help simplify decision-making:

- If two operating departments use two different approaches to defining customer addresses, and management needs data predicting customer churn by geographical area—the "owner" can determine which geographical data will be used in the analysis.
- An "owner" can also determine how to deal with data gathered from multiple external and unstructured sources (e.g., electronic forms, phone, text messaging, and email) and multiple audiences—such as health professionals and patients). In this example, if the language used by patients is less standardized than that used by health care professionals, the owner can identify how to and who can perform a mapping of one audience to the other.

Key takeaways/ recommendations:

- Data ownership is a complex responsibility; but ownership is critical for leveraging the potential of data-driven digital economy.
- Ideally, whomever owns data must understand and be held accountable for: (1) the processes via which data are generated; and (2) the technical and business owners of these processes.

Consideration #2: Artificial Intelligence and the Need for Good Data

As firms increasingly adopt information and communication technologies (ICTs) to seek efficiencies in business processes, artificial intelligence (AI) stands to become one of industry's most disruptive forces.

In fact, both the ability to obtain data about customers (from IoT-enabled devices and machines), together with the ability to *program AI to analyze the data*, have become important tools that businesses use to compete in an increasingly global economy.

As one example, AI is being used in physical security situations—such as where an individual responsible for monitoring several video cameras may become fatigued and unable to effectively view multiple monitors at the same time. AI can take input from multiple security cameras simultaneously and determine whether there may be a threat—and if it "sees" a warning sign, it will alert human security officers, who can then manage the issue at hand.

Outside of business benefits, AI also enables organizations to leverage data in new and innovative ways, coming up with life-saving solutions to dramatically improve:

- The quality of our healthcare;
- Human mobility, by managing city traffic better; and
- The ways we detect storms, hurricanes and tornadoes, to notify residents earlier.

THE NEED FOR GOOD DATA

In instances like the ones above, the foundation for AI is vast amounts of quality data. In fact, the increased availability of good data will be the single biggest contributor to increasing significant AI.

Currently, businesses collect data through a variety of channels—including applications (apps) on consumers' smartphones, where consumers provide information in exchange for usage of the app. This data serves as "business intelligence," with the business benefit of increasing returns on the data collected.

But with AI, smartphones turn consumers into something more: walking and talking "sensors" from which data can be collected and pumped into AI, from which new solutions are created.

Recently, major AI advances have been fueled by advances in data sets (related sets of information that can be manipulated as a unit by a computer), which hold significant potential to further boost economic growth.

To take advantage of this technology, individual businesses and entire sectors alike need enough data for analyzing—so they can build models and run machine-learning AI to solve problems and develop new solutions.

This makes the case for quality open data (that is, ensuring structured data is machine-readable, freely shared, used and built without restrictions) ever more important. In fact, the AI boom is as much about the availability of massive data sets, as it is about AI—because the bigger the data sets, the smarter the AI.

CONCERNS ABOUT AI

There is some concern that AI/advanced-learning machines may replace low-skill jobs. However, Gartner suggests that by 2020, AI-related job creation will actually surpass job losses. Moreover, AI will be able to work collaboratively with human professionals to solve intensely complex problems.

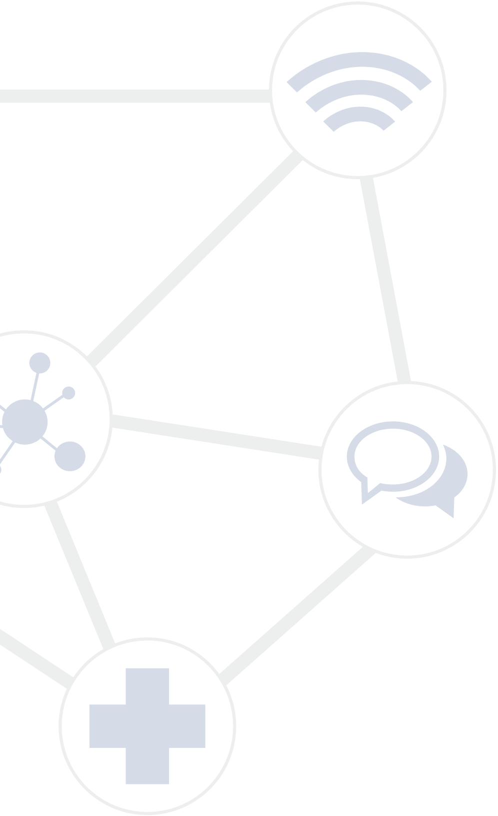
Another concern, particularly as the prevalence of AI increases in all facets of business operations, is regarding the underlying ethics and bias within AI models. While not dismissing AI's positive progress, there have been some examples where this technology has been used to perpetuate an implicit bias—with negative consequences.

To enable Canadian businesses and academic institutions to continue to build and lead in developing these technologies, a framework which supports public trust is imperative. The need is for clear guidelines around the building of this technology, and around disclosure, to ensure the public trust is not harmed and progress is not slowed.

The European Commission proposed the development of AI Ethics Guidelines by the end of the year. The topics to be included in the guidelines are future of work, fairness, safety, security, social inclusion, algorithmic transparency, privacy, dignity, consumer protection and non-discrimination.

AI is only as good as the data inputs; and as such, bias can surface in various ways. For example, sometimes the training data is insufficiently diverse, prompting AI software to make guesses based on what it "knows." Even when the data accurately mirrors, in reality the algorithms may still get the answer wrong—for example, incorrectly identifying a particular nurse in a photo or text as female, simply because data shows that fewer men are nurses.

In some cases, the algorithms are trained to learn from the people using the software and, over time, pick up on the biases of the human users.



Key takeaways/ recommendations:

- The foundation for AI is vast amounts of quality data. However, with a highly restrictive data policy environment that goes against open data, Canada may not be able to take advantage of all that AI promises. (For example, new businesses may become increasingly difficult to get off the ground if they have limited access to quality data.)
- Meanwhile, Canadian businesses and academic institutions need a framework that enables them to continue to build and lead in developing AI technologies, while also supporting public trust and ensuring progress is not slowed.
- As such, a national data strategy that supports AI should include guiding principles around two things: (1) transparency of the AI model; and (2) furthering controls already in place, to protect from bias.

Consideration #3: Fifth Generation (5G) Networks

IoT, smart cities, and automated and connected vehicles are expected to create vast amounts of data. As a result, modern hyper-connected networks will be required for transmitting that data to needed to perform tasks and provide business value.

Fifth generation (5G) networks will provide that solution, as 5G is predicted to revolutionize the way we use and leverage technology.

By delivering faster transmission speeds to support the broader deployment of hyper-connected devices, from autonomous vehicles to city infrastructure, 5G will:

- Make possible new classes of advanced applications,
- Foster business innovation, and
- Spur economic growth.

Ultimately, the combination of 5G networks (providing the backbone for data transmission)—along with widespread sensor placement and sophisticated data analysis techniques leveraging AI—will enable applications to aggregate and develop new innovative solutions to societal problems, impacting everything from healthcare to mobility to agriculture.

Key takeaways/ recommendations:

- Governments should allocate adequate funding to build a test-beds-and-innovation corridor for 5G wireless technology.
- Governments should also incentivize the roll-out of 5G networks through program funding and changes in tax policies, providing Canadians with the backbone required to engage in a data-driven digital economy.

Consideration #4: Trans-Border Data Flows

Businesses today rely on the free flow of data from diverse participants to reach customers, create jobs, and grow the economy.

Indeed, "data flows" are critical to the growth of the technology industry and many other organizations—both locally and internationally.

Meanwhile, with the liberalization of global trade, economic interdependence between countries has grown.

Thus, data flows require an international dimension—which presents both a huge challenge and opportunity for policymakers to build new economic agreements between countries, and to increase global trade.

DATA FLOWS VS. PHYSICAL TRADE

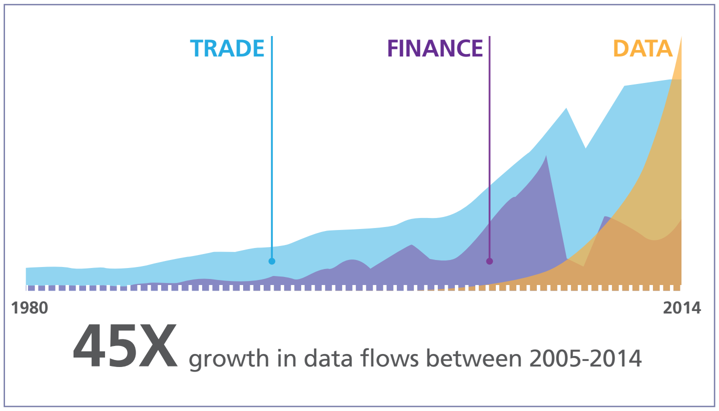
Recent news on global trade has tended to focus on protectionist measures and diplomatic tensions. These challenges have raised concerns over growth and jobs across the world.

Yet what is often lost in the current discussions is that we are entering a new era of trade—an era in which data flows are becoming more important than physical trade.

Consider the following:

- From 1986-2008, global trade in goods and services grew at more than twice the rate of the global economy. In recent years, however, growth in this more traditional type of trade has barely exceeded global GDP growth.
- At the same time, digital flows have been booming. According to Cisco, the amount of cross-border bandwidth used worldwide grew 90-fold between 2005 and 2016—and this is expected to grow an additional 13-fold by 2023. Leveraging a data-driven digital economy is all about transmitting vast amounts of data, and leveraging data to boost other flows, especially making services more tradable—from engineering, to software, to communications, to transportation

In fact, the future of trade is going to be increasingly dependent on data. The chart below shows how quickly data flows have increased in recent years, noting 45 times the growth between 2005 and 2014:



Source: McKinsey Global Institute

Key takeaways/ recommendations:

- Canada will not unlock the economic potential of the data-driven economy without the free flow of trans-border data. In fact, by not considering it, we will see a reduction of foreign investment in Canada that: (1) discourages trade; and (2) encourages innovative Canadian startups and entrepreneurs to launch their business in other regions of the world.

- A national data-driven digital strategy must recognize the extent and diversity of data traded or exchanged across borders.

- However, trans-border data flows must also recognize the need for assurances for citizen privacy and data security. Indeed, without trust in technology, consumers may avoid participation in the digital economy.

Consideration #5: Quantum Computing

Companies are racing to create the next generation of supercomputers—also known as quantum computers.

This type of technology will help solve life's most complex problems and mysteries regarding the environment, aging, disease, war, poverty, famine, the origins of the universe and deep-space exploration.

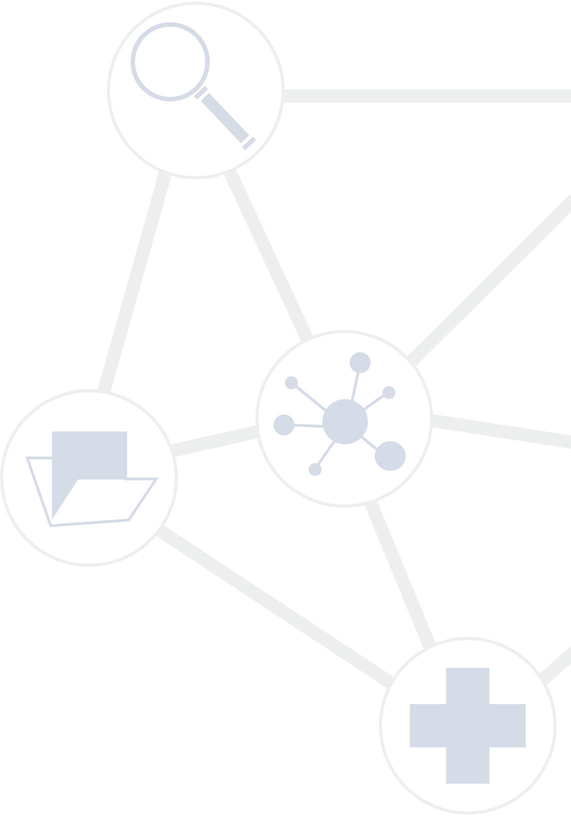
Quantum computers will also be the future powerhouse of all AI systems, acting as the brains of these super-human machines.

But despite its promise, quantum computing holds an inherent risk. For example:

- What will happen after the first quantum computer goes online, making the rest of the world's computing obsolete? Current levels of encryption considered to be logically unbreakable today will be "destroyed" by quantum computers decrypting today's standard, much the same way the earliest computers were used to decrypt German Enigma machines.
- How will existing architecture be protected from the threat that these quantum computers pose? Considering that the world lacks any formidable quantum-resistant cryptography (QRC), how will we protect our assets from people/institutions hellbent on using quantum computers to hack the world's most secretive and lucrative information?

Key takeaways/ recommendations:

- Quantum computing presents an exciting facet to how Canada uses data.
- However, a national data-driven digital strategy must consider the increasing need for Quantum-Resistant Cryptography—that is, algorithms to help secure against attacks by quantum computers.



Consideration #6: Shifting from Open Data to Integrated Data Sharing

Data is accumulating exponentially. The world developed more data in 2017 than in all of human history to date. But what is more important than the ability to create data is the ability to distribute and share data—thereby driving collaboration and innovation.

Governments at all levels have been determined to open access to their various data sources, making that data available for use in academic or commercial settings.

However, with slower-than-expected adoption of open data access across all levels of government, many believe that Canadians have not experienced the real or full potential that open data initiatives can bring.

OPPORTUNITIES FOR INTEGRATED DATA SHARING

Imagine the types of services that governments and industry could create via bi-directional, integrated data sharing—an ecosystem environment where:

- Smartphones are communicating with city-based infrastructure; which is
- Communicating to public transportation infrastructure; which is
- Relaying traffic patterns to our mapping applications, so we can avoid traffic or pick the fastest routes home.

All of this data could be collected, shared and integrated between industry and government, enabling things like:

- The assessment of real-time environmental effects of traffic (CO2);
- Re-sequencing of traffic lights to improve flow and limit collisions and the potential for cyclists and pedestrians to be struck; and
- Real-time information-sharing with connected vehicles.

Moreover, if this information is shared publicly, innovators will be able to develop new applications, spurring downstream economic benefits.

Key takeaways/ recommendations:

- Ultimately, data should be as open and available as possible. However, governments need to engage industry players of all sizes and from all sectors, on how Canadians can leverage and combine data sets to spur real innovation.
- A national data-driven digital strategy should ensure that data is available to anyone and everyone, with the caveat that it be refined for the community to use it effectively.
- More specifically, governments should ensure that: (1) data available is useable, structured, scrubbed, and analyzed in a way that makes sense for businesses to drive innovation; and (2) vast amounts of unstructured data are correlated, allowing for industry and academic players to leverage it to develop new solutions.

Consideration #7: Digital Identities

Canada is undergoing a technology transformation where people's physical and digital lives are combining into a single, integrated modern way of living—also known as a "digital identity."

Businesses have already begun to use identity to transform and personalize users' experiences as they interact with products, stores and services. For example, fitness wearables or healthcare monitors can offer personalized functionality; and with AI, a jogger's heart attack could be predicted weeks ahead of the event occurring, thereby saving money for the healthcare system while significantly benefitting people's lives.

This "new world" needs a new model for digital identity: one that enhances individual privacy and security across the physical and digital world.

Such a model will allow individuals to manage their own digital identity—providing increased individual control and privacy to consumers, while also providing organizations with greater visibility into consumer preferences.

Digital identity management rules will:

- Govern what businesses can and can't do online;
- Manage how well our enterprises can serve us, and how and to what extent businesses can collect and use the data they collect; and
- Protect governments' and businesses' reputations by preventing breaches.

Blockchain, the distributed ledger system, can be used as the process for managing and securing digital identities through authentication and encryption. Its end goal is to protect organizations' reputation from breaches of privacy or downtime, by accurately authenticating and authorizing who gets access to data.

Essentially, blockchain represents a new day in digital identity management: one where identity owners have more control of their most personal information, and where businesses can worry less about managing it.

Key takeaways/ recommendations:

- Organizations will not fully benefit from a data-driven digital economy without a scalable and streamlined digital identity strategy that enables businesses and consumers to interact with one another (e.g., through technologies such as biometrics to manage our identities and our health).
- If Canadian firms are not correctly authenticating digital identities, they will continue running the risk of data breaches. Technologies like blockchain can help with this.
- A well-developed digital identity management framework will leverage security to control access and use of our data for the things that are important to us.

Consideration #8: Data Protectionism

The McKinsey Global Institute estimates that cross-border flows of goods, services and data added 10 percent to global gross domestic product from 2005 to 2015—with data providing one-third of that increase.

In fact, the share of data's contribution to trade seems likely to rise; while conventional trade in products has slowed, digital flows have surged.

Yet while the world moves towards economies and sectors that are increasingly dependent on data to develop efficiencies, many countries are imposing or increasing restrictions—referred to as "data localization measures"—on trans-border data flows

DATA LOCALIZATION MEASURES

Today in parts of Canada, exporting health data of individuals to a foreign jurisdiction is restricted because of provincial privacy laws.

Here are a few other examples of data localization measures internationally, as well as their financial impacts:

CHINA

In China, data localization restrictions are severe. Citing concerns of sovereignty and national security, China's Great Firewall has long blocked most foreign web applications, and a cyber-security law passed in 2016 also imposed rules against exporting personal information.

The US Chamber of Commerce suggests that data localization will reduce Chinese GDP by a total of between 1.8 percent and 3.4 percent by 2025. Meanwhile, the Organisation for Economic Co-operation and Development (OECD) predicts a GDP of USD$53.8 trillion in 2025, which would cost China between USD$969 billion and USD$1.8 trillion.

UNITED STATES

Rules guaranteeing trans-border data flows were included in the Trans-Pacific Partnership (TPP). However, with the election of President Donald Trump, the US has pulled out of the TPP. The remaining 11 TPP countries retained the data provisions when they revised the text of the agreement.

EUROPE

Europe has traditionally had a very different philosophy towards data and privacy, taking a more sensitive approach to data protectionism. This is often attributed to historical events, including lingering memories of surveillance by the SS during World War II.

The European Centre for International Political Economy, a think-tank, calculates that from 2006 to 2016, the number of significant data localization measures in the world's large economies nearly tripled from 31 to 84.

According to the McKinsey Global Institute, curbs on moving personal data from the European Union, even to other member states, is said to reduce EU GDP by half a percent. Based on World Bank data from 2016, the EU's GDP was USD$16.5 trillion, and this half percent cost the EU some USD$82 billion in GDP.

The EU's new General Data Protection Regulation (GDPR), which came into force on May 25, 2018, imposes a long list of requirements on companies processing personal data—with lack of compliance resulting in extremely hefty fines up to €20 million (or 4% of the previous year's revenue).

In principle, GDPR can be compatible with encouraging trans-border digital flows. However, there are discrepancies between the goals of the EU trade policy groups, and privacy and data protection groups respectively.

IMPACT ON INDUSTRY

Protectionist restrictions are resulting in the following:

- Such policies cause industry players to incur extra costs, such as setting up local data storage and segregating some information from the rest of their operations.
- Blocking data flows also silos data into multiple digital sets—with each set having a different set of domestic laws and regulations, increasing complexity and limiting businesses' capacity to share and leverage data to improve processes.
- Moreover, because limits on data transfers impede the development of good structured data company- or industry-wide, this has made it more complex for the ICT industry to offer efficient and effective services to clients who wish to leverage AI and analytics.

And as the whole economy in all sectors becomes more data-dependent, the cost of blocking those flows increases.

(cont'd on next page)

Key takeaways/recommendations:

- This highlights the need for a whole-of-Canadian-government approach to setting data policy.
- By extension, advanced economies should unite behind a set of balanced rules on data.

Consideration #9: Data Residency and Sovereignty

Governments at all levels want to provide citizens the certainty that their personal data is protected from unwanted access—not only from nefarious attackers, but also from other governments and agencies (whether accessed through legal or back-door channels).

From a public policy perspective, this has led some governments worldwide to mandate "data residency"—essentially, ensuring that all data remain resident within their own jurisdiction, believing that doing so provides an additional layer of security and protection from unauthorized access by foreign governments, businesses or law enforcement.

However, requiring that the storing of Canadian data is done on Canadian soil is a simplistic political approach to appeasing the public's need for security. Although policy makers assert that residency is the best possible way to protect data—especially since the United State's Freedom Act/PATRIOT Act was passed—residency does not do a lot for security.

That said, the EU has recognized the importance of data flows, and have drafted the *Free Flow of Data Regulation* which is about removing national barriers to non-personal data flow within the EU (personal data is already subject to free movement within the EU under the GDPR). They recognized that data can create significantly added value to existing services and facilitate entirely new business models and that taking away obstacles to data mobility can generate an additional growth of up to 4% GDP by 2020 (Deloitte).

In fact, the physical location of data has little to no impact on threats propagated over the Internet. This is because Internet-connected systems expose an organization to a broad threat space, which are propagated from any location in the world. As such, whether data is housed in Canada, Iceland or Romania, this makes little difference to hackers. (Not to mention, many data breaches are inadvertently caused by employees, such as through e.g., phishing.)

But perhaps more important to this argument, the Internet is routed through exchanges throughout the world, seeking the shortest possible route between points A and B. Most Domain Name Systems (DNS) routers, resolvers and hosts are housed in the US—and Canada's Internet infrastructure is intimately linked to U.S. networks. Many networks favour north-south connections, pushing Canadian data flows toward key American routing hubs in New York, Chicago, Seattle or California.

When using these services, Canadians likely recognize the fact that their data leaves exclusive Canadian jurisdiction and is exposed to America. However, they may be surprised to learn that when accessing Canadian sites, their data often still flows through the United States. As most of the Internet's infrastructure runs through the US, even communications beginning and ending in Canada are often routed through America.

(cont'd on next page)

Key takeaways/recommendations:

- Ultimately, data residency is a jurisdictional issue—not a security issue.
- While some parties strongly believe data residency is key to maintaining future digital sovereignty, many believe that encrypting data or leveraging blockchain/cybersecurity measures—thereby limiting unauthorized access—are better alternatives to requiring residency.
- There is no one-size-fits-all type of solution to this argument. Some data will be more sensitive and should be more secure, while other data sets should be publicly accessible. Regardless, a national data-driven digital strategy should incorporate all these views.

Consideration #10: Data Security and Privacy

Managing data security may become an even greater policy imperative—particularly as the IoT, connected and automated vehicles, and smart cities connect data sets in real-time.

Indeed, the privacy challenges posed by new technologies are significant, as is the erosion of trust in the digital economy.

OBTAINING CONSENT AND TRUST

Traditionally, to collect consumer data, enterprises have been required to seek individuals' consent/agreement in writing. This has traditionally been the manner which businesses provide fundamental protections of consumers' privacy. In many circumstances, individuals are willing to exchange private information to access services or other information. Organizations provide consumers with information to help them make an informed decision about how they wish to share their personal data.

With digital uses of data, consumers rarely make their way through the information, opting more often to just "click-through" the terms of the agreement. In certain circumstances, this is the result of trust between the consumer and the company, hence an expedited process.

That said, an erosion of that trust can often cause individuals to review their consent and seek the removal of their personal information in the hands of the company.

PRIVACY CONCERNS IN HEALTH

In the health sector, privacy is of concern. Unfortunately, privacy and confidentiality-related issues have been perceived by many as an impediment to many large-scale digital health initiatives in Canada.

As a new national data strategy is crafted, it is important that health risks and privacy risks be seen in their proper contexts.

Better health-data sharing, as mentioned above, relies particularly on the sharing of patient health data within the circle of care. This is a safety and quality-of-care issue—and our healthcare system's default operating procedure should be to share personal data to ensure patient-safe, high-quality care delivery.

Likewise, the operation of a Learning Health System—and the efficiencies and health benefits that arise from one—relies on broad sharing of de-identified, person-centric data. However, in the face of public health emergencies, or to protect an individual's personal safety, it must be possible to re-identify individuals using some form of ID-escrow process.

Privacy risks are genuine, and the operation of the health system must protect the confidentiality of personal health data. But the risks related to privacy are not necessarily of the same magnitude as the health risks that could arise from not having access to data (through large-scale, interoperable, health-data sharing infrastructures).

SECURITY CHALLENGES AND IMPACT

The security challenges posed by collecting and controlling data have increased exponentially in recent years, particularly as the value of data has increased.

As such, innovative businesses are increasingly exposed to dishonest practices aimed at misappropriating trade secrets and intellectual property (IP).

Cybercriminals, who are increasingly well-organized, pose significant risks and have caused economic harm undermining organizations' reputation and financial viability (e.g., Equifax, Uber, TJX, Yahoo), with consequences including:

- Damaged revenues through the disruption of business operations,
- The undermining of a firm's reputation,
- Negative impact/influence on the stock prices of publicly traded companies, and
- Disrupting lines of business through corporate espionage.

Meanwhile, technology-enabled theft of IP and trade secrets have been continuously escalating: these attacks were estimated to make up 25% of all cyber-attacks across all sectors and up to 94% of all cyberattacks in the manufacturing sector in 2016.

The cost of industrial IP and trade secrets theft is expected to cost from 1-2% of GDP annually and result in a global loss of competitiveness, reduced R&D investments and jobs.

Without effective legal and technological means for protecting IP and trade secrets, incentives to engage in innovation-related cross-border activity are undermined.

These growing attacks are being motivated more and more by state-affiliated actors.

MINIMIZING RISK

There are several ways that public- and private-sector organizations are working to minimize security risks pertaining to data:

- Governments at all levels in Canada are currently reviewing how to combine and merge data sets from different departments, since they see its potential for better serving Canadians. One way to avoid any potential implications is to anonymize the data, removing personal information or personally-identifiable information (PII). The concern with this practice is that when combining data sets, it may become increasingly easy to identify an individual without any PII.
- On the industry front, for the purpose of analytics and reporting, businesses where feasible, could remove all personal and business-identifiable information from data that would be accessible to employees or partner organizations. What then remains are the data elements required for key performance indicator (KPI) calculations and other more generic informational dimensions (e.g., city, province, business sector). This can lead to an active approach to anonymization that not only protects customer and citizen information, but also protects companies and employees from unauthorized data usage. All of this to protect both consumer and business privacy, while ensuring businesses are less susceptible to data breaches.
- Meanwhile, the Office of the Privacy Commissioner of Canada, as well as Provincial Commissioners, have called on businesses to create a "Privacy-by-Design" approach to product design and development. When ideating and designing new data-driven solutions, one of the ICT industry's core principles includes ensuring that the privacy of merchants and consumers is maintained in accordance with privacy laws and regulations. This includes ensuring that no personal identifiable information (PPI) is used or disclosed without consent, as required by the Personal Information Protection and Electronic Documents Act (PIPEDA).

(cont'd on next page)

Key takeaways/recommendations:

- Governments must come to terms with the fact that connecting data sets, and opening up access and use, exposes data to some degree of digital security risk; and when personal data is involved, this exposes data to potential privacy challenges as well.

- In developing a national data-driven digital strategy, address data security and management as an economic and social risk, rather than solely as a technical issue. In other words, consideration should be given to the potential economic and social consequences of a possible security incident affecting the availability, integrity or confidentiality of data.

- Better data protection policies, security measures and technologies can be leveraged to protect Canadians' data. A national data-driven digital strategy should: (1) evaluate the potential benefits vs. privacy risks of sharing date (e.g., health data); and (2) include standards for access, encryption and anonymization.

- In addition, the Government needs to lead a dialogue on "data ethnicity." While access to data—such as health or smart city data—can have enormous benefits, access to the same data can be used by actuaries to discriminate against identifiable demographics to classify groups.

CONCLUSION

Indeed, Canada and the world are benefiting from significant technological and human advancements that continuously re-define and change our quality of life for the better.

We already live in an environment that enables blockchain to manage our identities, contracts and business information; and where data collected from automated vehicles and smart cities will solve most traffic issues and increase rider safety, saving countless lives.

Taking things further, a digital data-driven economy is one where:

- We can leverage quality data sets to inform AI and machine learning to develop solutions for countless industries—from agriculture and farming, to mining and resource extraction—all the while, improving worker safety and overall efficiency.
- 5G networks can transmit the incredible amounts of data generated and rely on AI to come up with novel solutions to society's toughest challenges.

All of these advancements are going to be largely dependent on data.

ITAC and its members are positioned to help enable the advancement of industries via technology. As such, ITAC strongly recommends the Federal Government, in partnership with provinces and territories:

- **Lead a national dialogue to shape data governance**, based on agreed-upon principles that can both ensure trustworthiness and unlock the economic potential; and
- **Develop a national data-driven digital strategy** that both takes into account individual and business needs around the access to and protection around data, while allowing for growth and innovation.

GLOSSARY

Analytics
Information and insights that come from the analysis of data or statistics.

Artificial Intelligence (AI)
Umbrella term for machines that perform functions, mimicking how humans would carry out the same tasks.

Blockchain
A "distributed ledger technology" (DLT) primarily used to verify transactions. Within digital currencies, this technology is also used to digitize, code and insert practically any document into the blockchain—creating a record that cannot be changed, thereby verifying its authenticity.

Data flow
The route taken by data within a device, network, or organization, as it moves from its source to another source or data user.

Data governance
The overall management of data used in an organization—including (but not limited to) its availability; where it is sourced, collected or generated; when and how it is analyzed, manipulated, shared or transformed; and its security.

Data liquidity
The ability of patient data to move through a healthcare system securely and effectively.

Data localization
The act of storing data on a device that is physically within the country where the data was generated.

Data protectionism
The process of protecting important information from being corrupted, compromised, or lost altogether.

Data sets
A collection of related sets of information. Each set is composed of separate elements that can be manipulated as a unit by a computer.

Data sovereignty
Refers to digital data that is subject to the laws of the country in which it is located. E.g., if data is stored within Canada, it should fall within Canadian privacy laws. If that data flows within the country, those privacy laws apply. If that data travels outside Canadian borders, Canadian privacy laws no longer apply.

Digital identity
An online identity adopted or claimed in cyberspace by an individual, organization or electronic device.

DNS
An acronym for Domain Name System. This refers to a service for accessing a networked computer by name, rather than by a numerical (IP) address.

Encryption
The manipulation of data, preventing others from accurately interpreting and "hacking" it.

Internet of Things (IoT)
An ecosystem of connected devices—ranging from smartwatches to smart refrigerators and HVAC systems—that can transfer data over a network without human-to-computer interaction.

Machine Learning (ML)
An application (or subset) of AI that allows computers to train and learn for themselves, using data that they have been fed or given access to. Essentially, ML is a reality where computers could perform any task that a human can, and typically more efficiently and effectively.

Personally identifiable information (PII)
Information that can be used to uniquely identify, contact or locate a single person.

Structured data
Information with a high degree of organization. This kind of data is readily searchable by "machines" or search engines, making information much easier to deal with using computers. Example: spreadsheets.

Unstructured data
Information that is not easy to machines to search, understand or organize. Example: the contents of an email inbox.

REFERENCES

ARTICLES

Big data, big responsibilities. Organisation for Economic Co-operation and Development (OECD). 2018.
http://oecdinsights.org/2018/03/30/big-data-big-responsibilities/

Data-protection laws must be extended to political parties. Globe and Mail. 2018.
https://www.theglobeandmail.com/opinion/article-data-protection-laws-must-be-extended-to-political-parties/

Exploring the new data economy. LinkedIn. 2017.
https://www.linkedin.com/pulse/exploring-new-data-economy-michael-dingle/

For AI, good quality data is a necessity: ABB's Guido Jouret. Livemint.com. 2018.
https://www.livemint.com/Companies/3ihXengq5UEuXQmLEFx6tO/For-AI-good-quality-data-is-a-necessity-says-Guido-Jouret.html

Here are 4 building blocks for the new era of trade which will benefit everyone. World Economic Forum. 2018.
https://www.weforum.org/agenda/2018/05/creating-a-better-global-trade-system

Is Big Data Finally Changing Health Care? Fortune.com. 2018.
http://fortune.com/2018/03/20/big-data-finally-changing-health-care/?utm_medium=social&xid=soc_socialflow_twitter_FORTUNE&utm_source=twitter.com&utm_campaign=fortunemagazine

Labour productivity is Canada's 'Achilles heel': Scotiabank CEO. CTV News. 2016.
https://www.ctvnews.ca/business/labour-productivity-is-canada-s-achilles-heel-scotiabank-ceo-1.2855926

Microsoft will invest $5 billion in IoT. Here's why. Microsoft.com. 2018.
https://blogs.microsoft.com/iot/2018/04/04/microsoft-will-invest-5-billion-in-iot-heres-why/

Sidewalk Labs aims to address privacy concerns in designing high-tech Toronto neighbourhood. Globe and Mail. 2018.
https://www.theglobeandmail.com/canada/toronto/article-sidewalk-labs-hadnt-foreseen-data-concerns-in-designing-high-tech/

Why "Data Ownership" Matters. CTOvision.com. 2017.
https://ctovision.com/data-ownership-matters/

You have my data, where's my access? Healthcare Information Management & Communications. 2015.
http://www.healthcareimc.com/main/you-have-my-data-wheres-my-access/

You may have heard data is the new oil. It's not. World Economic Forum. 2018.
https://www.weforum.org/agenda/2018/01/data-is-not-the-new-oil/

NEWS RELEASES

Gartner Says By 2020, Artificial Intelligence Will Create More Jobs Than It Eliminates. Gartner. 2017.
https://www.gartner.com/newsroom/id/3837763

Researchers map the Internet's "boomerang routes" where data transfers between Canadians move through the US, increasing exposure to state surveillance. CIRA. 2015.
https://cira.ca/researchers-map-internet%E2%80%99s-%E2%80%9Cboomerang-routes%E2%80%9D-where-data-transfers-between-canadians-move-through-us

OTHER

2018 Technology Industry Outlook. Deloitte. 2018.
https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/technology-industry-outlook.html

Building a European data economy. European Commission. [2017].
https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

The city/suburb contrast: How can we measure it? StatCan. 2014.
https://www.statcan.gc.ca/pub/11-008-x/2008001/article/10459-eng.htm

Declaration on Transborder Data Flows. Organisation for Economic Co-operation and Development (OECD). 1985.
http://www.oecd.org/sti/ieconomy/declarationontransborderdataflows.htm

The Learning Health System Series. National Academy of Medicine. Date not available.
https://nam.edu/programs/value-science-driven-health-care/learning-health-system-series/

WHITE PAPERS/REPORTS

A Call to Action to Protect Citizens, the Private Sector and Governments. Organization of American States (OAS). 2018. http://www.oas.org/en/sms/cicte/awswhitepaper.pdf

Data Breach Investigations Report 2017. Verizon. 2017.
https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Data management and use: Governance in the 21st century - a British Academy and Royal Society project. The Royal Society. 2017. https://royalsociety.org/topics-policy/projects/data-governance/

Data residency: AWS policy perspectives. Amazon Web Services. 2018.
https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats. CREATe.org and PricewaterhouseCoopers LLP. 2014.
https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf

The Global Risks Report 2018. World Economic Forum. 2018.
http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

The Internet of Things: Seizing the benefits and addressing the challenges. Organisation for Economic Co-operation and Development (OECD). 2016.
http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En

A National Data Strategy for Canada: Key Elements and Policy Considerations. Centre for International Governance Innovation. 2018. https://www.cigionline.org/sites/default/files/documents/Paper%20no.160_3.pdf

Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II. Center for Strategic and International Studies. 2014.
https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

The Developing a Data-Driven Digital Economy in Canada Report is prepared by Information Technology Association of Canada (ITAC).

For inquiries about this Report, please contact: Andre Leduc, Vice President, Government Relations and Policy, ITAC at aleduc@itac.ca.

Written inquiries should be directed to 1120-220 Laurier Avenue West, Ottawa, ON, K1P 5Z9.