ontario chamber of commerce

In Data We Trust

Unlocking the Value of Data in Ontario

Claudia Dessanti
Senior Policy Analyst, Ontario Chamber of Commerce

TABLE OF CONTENTS

GLOSSARY

ALGORITHM: a procedure that a computer uses to solve a problem.

APPLICATION PROGRAMMING INTERFACE (API): mechanisms that allow for the secure sharing of data across parties.

ARTIFICIAL INTELLIGENCE (AI): the ability of a machine to perform tasks that normally require human intelligence, such as visual perception, speech recognition, and decision-making.

BIG DATA: large amounts of structured and unstructured data. Big data is often defined using the three Vs: volume, velocity at which it is collected, and variety of data points.

BIOMETRICS: (computer security) authentication techniques that rely on physiological or behavioural human characteristics, such as fingerprints, facial recognition, typing rhythm, and voice.

CIVIC DATA TRUST: an independent entity given responsibility for controlling, managing, and making publicly accessible data that could be considered a public asset.

CLOUD SERVICES: facilities managed by third parties that store and process end-user data while providing data management services over the internet.

CODE OF PRACTICE: specific guidance intended to complement regulation or laws by providing details on how to comply. In this report, 'code of practice' is used interchangeably with 'industry standard.'

CYBERSECURITY: protection against unauthorized access to information stored electronically.

DATA ECONOMY: the economic value created by organizations engaged in the retrieval, storage, and analysis of big data at high speeds using sophisticated software and other tools.[1]

DATA LOCALIZATION: a requirement that organizations store and process data within certain borders.

DATA PHILANTHROPY: the act of sharing private data assets to serve the public good.

DATA PORTABILITY: allowing individuals to access their personal information in machine-readable formats and share that data with other organizations.

DATA SHARING: when an organization or part of an organization makes its datasets available to researchers, other organizations, or other groups within the same organization.

DATA SHARING AGREEMENT (DSA): contracts that outline the terms and conditions associated with sharing of health data.

DIFFERENTIAL PRIVACY: a mathematical approach to data privacy that seeks to protect individual identities while preserving the ability to perform statistical analysis on the larger dataset. This is typically done by adding randomness or noise to the data.

ELECTRONIC HEALTH RECORD (EHR): a digital lifetime record of a patient's health history and care, with information from a variety of sources (including hospitals, clinics, doctors, pharmacies, and laboratories), designed to facilitate the sharing of health data across the continuum of care.[2,3]

ELECTRONIC MEDICAL RECORD (EMR): an individual patient record created by a health care provider following specific encounters with patients. EMRs can serve as a data source for an EHR.[4]

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA): legislation governing privacy and access to information held by public institutions in Ontario.

GENERAL DATA PROTECTION REGULATION (GDPR): guidelines for the collection and processing of personal information of individuals who live in the European Union.

HEALTH DATA: patient-, system-, and population-level information related to health care delivery, status, and outcomes.

HUMAN-IN-THE-LOOP: AI models that involve human oversight and/or intervention.

INDUSTRY STANDARDS: see 'codes of practice.'

[1] Digital Reality. 2018. The Data Economy Report 2018. *https://www.digitalrealty.com/data-economy.*

[2] eHealth Ontario. "What's an EHR?" *https://www.ehealthontario.on.ca/en/ehrs-explained.*

[3] Office of the Auditor General of Canada. 2010. "Electronic Health Records in Canada–An Overview of Federal and Provincial Audit Reports." *https://www.oag-bvg.gc.ca/internet/English/parl_oag_201004_07_e_33720.html.*

[4] Jamie L. Habib. 2010. "EHRs, Meaningful Use, and a Model EMR Managed Care Matters." Drug Benefit Trends. 22 (4): 99-101. *https://www.patientcareonline.com/drug-benefit-trends/ehrs-meaningful-use-and-model-emr.*

GLOSSARY

INFORMATION PRIVACY COMMISSIONER OF ONTARIO (IPC): the agency that oversees Ontario's provincial privacy laws (PHIPA, FIPPA, and MFIPPA).

INTANGIBLES ECONOMY: an economy where competitiveness is driven by intangible assets, such as data and intellectual property, as opposed to physical or tangible assets such as labour and capital.

INTELLECTUAL PROPERTY (IP): a form of creative effort that can be protected through a trademark, patent, copyright, industrial design, or integrated circuit topography. [5]

INTERNET OF THINGS (IOT): objects, devices, and spaces connected to the internet.

MACHINE LEARNING (ML): an advanced subset of AI that empowers computer systems to learn by themselves using provided data to make predictions.

MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (MFIPPA): legislation that governs how municipal institutions must protect privacy when collecting personal information.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC): the agency that oversees federal privacy laws (PIPEDA and the Privacy Act).

OPEN CONTRACTING: the practice of publishing open, accessible, and timely information about the planning, decision making, scoring, and awarding of all government contracts.

OPEN DATA: data that is machine-readable, freely shared, used, and built on without restrictions. [6]

OPEN SOURCE: software for which the original source code is made freely available to developers and entrepreneurs.

PERSONAL HEALTH INFORMATION PROTECTION ACT (PHIPA): legislation governing the collection, use, and disclosure of personal health information in Ontario by doctors, hospitals, and other data custodians involved in the delivery of health care services.

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA): a federal privacy law that applies to the collection, use, and disclosure of personal information for commercial activities.

PRIVACY: protection against unwanted intrusion into people's communications, opinions, beliefs, and identities. Data privacy is concerned with how information is collected, shared, and used.

PRIVACY ACT: legislation that specifies individuals' privacy rights in their interactions with the Government of Canada.

PRIVACY BY DESIGN: an approach to data privacy that builds privacy protection into organizational systems at all stages of system development and in daily use. [7]

[5] Canadian Intellectual Property Office. "Glossary of Intellectual Property Terms." *https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr00837.html.*

[6] Government of Canada. "Open Data 101." *https://open.canada.ca/en/open-data-principles#toc94*. Accessed March 20, 2020.

[7] Datatilsynet. 2018. Artificial Intelligence and Privacy. *https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.*

EXECUTIVE SUMMARY

Data is rapidly becoming one of the most valuable resources in the modern economy and Ontario has the potential to benefit immensely from this transformation. However, along with its many social and economic benefits, the data revolution comes with certain risks, including the erosion of personal privacy, data security breaches, labour market disruption, ethical challenges, and increasing regional inequality.

Governments, businesses, and other stakeholders will need to foster an environment that encourages data-driven innovation while protecting against these risks. *In Data We Trust: Unlocking the Value of Data in Ontario* discusses how Ontario can achieve this with strong governance frameworks and stewardship from the organizations that collect, process, use, and share data. The report argues:

Privacy frameworks should protect individual rights while encouraging data-driven innovation. Ontario and Canada should retain their existing principles-based approach to privacy while reinforcing it with strong industry standards. Businesses and other organizations have an important role to play to ensure their own privacy practices enhance public trust.

Cybersecurity breaches are affecting organizations of all kinds. More can be done to build capacity and limit future attacks with stronger adoption of industry standards, information sharing, and best practices around risk assessments, staff training, technology adoption, and insurance.

Data sharing across silos is an opportunity to improve efficiencies and spur innovation across the economy. Organizations should collaborate on shared standards and infrastructure to enable data sharing across all sectors, including health care, without compromising privacy. Meanwhile, governments should improve the utility of their open data programs.

Artificial intelligence (AI) is a competitive advantage that Ontario should leverage deliberately. Going forward, the province must translate its research expertise into widespread adoption of the technology, prepare the workforce for an AI-driven economy, and mitigate ethical risks related to AI use.

The report contains a series of policy recommendations and organizational best practices to help position Ontario for data-driven success.

CHAPTER I

ONTARIO'S DATA-DRIVEN ECONOMY

Data is transforming our economy and ways of living. The fact that businesses collect and process data is not new; firms have always used data to forecast revenue, allocate resources, and develop new products and services. However, the sheer volume of data being collected is unprecedented, and the data organizations analyze is increasingly personal and sensitive, including geolocations, internet searches, and spending patterns. While data was once seen as a byproduct of transactions, it is now widely regarded as a strategic asset.

Data is often discussed in the context of the digital economy because it is technology that has enabled the large-scale collection, aggregation, storage, and processing of information. Artificial intelligence (AI) is critical to unlocking the advanced analytical powers of data. Data-driven technologies include social media platforms, wearable devices, autonomous vehicles, and smart sensors – to name just a few.

Yet, it is a mistake to think of data as simply being a technology-sector issue. Data is permeating every sector of Ontario's economy: health care, financial services, agriculture, manufacturing, retail, and beyond. In the future, as businesses adopt more digital technologies, data will continue to become an increasingly valuable resource.

AN AVERAGE DAY

To understand the myriad of ways data is transforming Ontario, consider the following hypothetical day. There is nothing exceptional about this story; it could apply to a resident in many cities and towns across the province.

YOUR ALARM WAKES YOU FROM A DEEP SLEEP. YOU ROLL OUT OF BED AND INTO THE KITCHEN TO PREPARE BREAKFAST: FRESH ONTARIO EGGS, PERFECTLY SCRAMBLED, WITH BACON AND AN APPLE.

Ontario's agricultural sector uses data to optimize resource allocation and improve cost efficiency across the food supply chain. Sensors collect information on soil nutrient content, equipment productivity, crop yields, bacteria, livestock health, and more.[8] Advanced data analytics is helping to manage some of the uncertainty that characterizes the agricultural sector.

YOUR KITCHEN IS EQUIPPED WITH A SMART REFRIGERATOR, WHICH ALERTS YOU THAT YOU ARE RUNNING LOW ON EGGS.

YOU USE YOUR VOICE TO ADD THE ITEM TO YOUR SHOPPING LIST BEFORE CHECKING THE FRIDGE'S SCREEN FOR ANY NOTES FROM YOUR FAMILY MEMBERS.

Smart fridges are one of many examples of Internet of Things (IoT) devices. IoT applications extend far beyond home appliances, providing solutions for supply chain management, facility maintenance, smart cities, environmental conservation, and more.

ALONG WITH BREAKFAST, YOU TAKE YOUR DAILY HEART MEDICATION.

Big data is also helping to reduce the cost of bringing new drugs to market. Pharmaceutical companies are using AI for drug discovery to more accurately predict whether a drug will be effective, thereby improving the success rates of clinical trial and reducing overall research and developments costs.

YOUR BREAKFAST ROUTINE IS NOT COMPLETE WITHOUT ACCESSING THE LATEST NEWS AND UPDATES ON YOUR TABLET.

YOUR NEWS FEEDS AND SOCIAL CHANNELS ARE CUSTOMIZED BASED ON THE TYPES OF CONTENT YOU HAVE ENGAGED WITH IN THE PAST.

THE ADVERTISEMENTS YOU SEE ARE ALSO ALIGNED WITH YOUR RECENT BROWSING AND ONLINE SHOPPING HABITS.

Technology companies deploy AI to provide their users with more personalized services. Based on patterns of online behaviour, they are able to infer users' demographic and other characteristics to provide them with more relevant information.

Similarly, retail companies use online activity and purchase histories to target their marketing and offer personalized discounts. The proliferation of online shopping has allowed the sector to collect more information than ever before.

ONE ADVERTISEMENT STANDS OUT TO YOU. AN ONTARIO-BASED INSURANCE PROVIDER IS OFFERING A NEW USAGE-BASED AUTO INSURANCE PLAN.

Insurance providers use data to lower costs and provide more customized products to their customers. For example, auto insurance providers are implementing usage-based insurance systems, which rely on in-car technology to monitor how customers drive and adjust premiums accordingly.

[8] The Refresh Working Group. 2018. Refresh: Food + Tech, from Soil to Supper. *http://refreshfoodandtech.com/wp-content/uploads/2018/11/refresh-report.pdf.*

CHAPTER I ONTARIO'S DATA-DRIVEN ECONOMY

AFTER BREAKFAST, YOU GET DRESSED AND RUSH OUT THE DOOR, BUT NOT BEFORE PUTTING ON YOUR WEARABLE FITNESS TRACKER. YOU FEEL OPTIMISTIC ABOUT REACHING YOUR DAILY STEP COUNT GOAL TODAY.

Wearable technology, such as fitness trackers and smart watches, are growing in popularity among Ontarians. These devices generate large amounts of data by tracking individuals' geolocations, energy usage, heart rates, sleeping patterns, and more.

YOU SPENT A LITTLE TOO MUCH TIME READING THE NEWS THIS MORNING AND MIGHT BE LATE FOR YOUR FIRST MEETING, SO YOU DECIDE TO USE A RIDE-SHARE SERVICE TO CUT DOWN ON TRAVEL TIME.

Ride-sharing platforms use historical and global positioning system (GPS) data to match drivers with riders and predict trip durations. The more these platforms are used, the more data they can feed into their algorithms, which improves performance.

THERE IS SOME LIGHT TRAFFIC ON YOUR COMMUTE.

Urban planners see data as the key to improving the efficiency and safety of transportation networks. Aggregated information on congestion, freight logistics, and passenger usage is used to inform transit planning, scheduled maintenance work, and new investments in infrastructure. More broadly, many municipalities in Ontario are integrating smart city solutions such as sensors to collect data that helps planners find efficiencies. Some examples include smart waste management, smart meters, smart street lighting, and smart parking management.

YOU ARE HAVING A PRODUCTIVE DAY AT WORK. AT LUNCH, YOU HEAD TO THE DOCTOR'S OFFICE TO DISCUSS THE RESULTS OF A RECENT X-RAY.

YOUR DOCTOR PULLS UP YOUR ELECTRONIC HEALTH RECORD AND EXPLAINS YOUR TEST RESULTS.

One of AI's emerging applications involves medical imaging services, where machine learning can help radiologists deliver diagnostics more quickly and accurately. AI's many applications in health care are discussed further in Chapter V.

Electronic health records (EHRs) can contain several pieces of personal information about patients, including their names, ages, addresses, health card numbers, previous lab results, allergies, and more. By allowing providers to track and share clinical data, EHRs help improve the continuity and overall quality of care.

YOU RETURN TO YOUR DESK AND CONTINUE WORKING AWAY UNTIL YOU GET A CALL FROM YOUR BANK.

Fraud detection is one of many ways the financial services sector uses advanced data analytics. Other use cases include portfolio analysis, predictive modeling, and stress testing.

THEY HAVE DETECTED AN ABNORMAL SPENDING PATTERN ON YOUR ACCOUNT AND WANT TO VERIFY A FEW RECENT TRANSACTIONS.

AFTER WORK, YOU SPEND SOME TIME WINDOW SHOPPING AT THE MALL, WHERE YOU BROWSE A VARIETY OF CONSUMER GOODS, INCLUDING APPLIANCES, CLOTHING, AND FURNITURE.

Manufacturers in Ontario use advanced manufacturing processes that incorporate data-driven technologies at every stage. Today's manufacturing facility, like the modern farm, uses digitally connected devices to continuously gather information that allows for improvements to preventive maintenance, inventory control, energy efficiency, and supply chain management.

SAFELY HOME AFTER A LONG DAY, YOU BEGIN TO PREPARE DINNER.

YOUR VOICE ACTIVATES A SMART SPEAKER AND YOU ASK IT TO PLAY YOUR FAVOURITE JAZZ ALBUM WHILE YOU UNWIND.

DATA IN NUMBERS

2.5 QUINTILLION

BYTES OF DATA ARE PRODUCED IN THE WORLD EVERY DAY.[9]

VOLUME OF DATA GENERATED PER MINUTE IN 2019:

- **188,000,000** EMAILS SENT
- **4,497,420** GOOGLE SEARCHES CONDUCTED
- **390,030** APPS DOWNLOADED
- **511,200** TWEETS POSTED[10]

$29-40 BILLION

CANADIAN INVESTMENT IN DATA AND DATA SCIENCE IN 2018 (80% FROM PRIVATE-SECTOR SOURCES).[11]

$4 TRILLION

VALUE OF THE WORLD'S FIVE LARGEST DATA-DRIVEN COMPANIES IN 2019.[12]

$166 BILLION

ESTIMATED GLOBAL SPENDING ON INFORMATION SECURITY SERVICES IN 2019.[13]

71% **OF FINANCIAL SERVICE FIRMS ARE INVESTING IN BIG DATA AND PREDICTIVE ANALYTICS.**[14]

[9] Mastercard. 2019. The Global Data Responsibility Imperative. *https://www.mastercard.us/content/dam/mccom/en-us/documents/global-data-responsibility-whitepaper-customer-10232019.pdf.*

[10] Domo. "Data Never Sleeps 7.0." *https://www.domo.com/learn/data-never-sleeps-7.*

[11] Statistics Canada. 2019. "The Value of Data in Canada: Experimental Estimates." Latest Developments in the Canadian Economic Accounts. Catalogue no. 13-605-X. *https://www150.statcan.gc.ca/n1/en/pub/13-605-x/2019001/article/00009-eng.pdf?st=Bouygwzw.*

[12] Robert Asselin and Sean Speer. 2019. A New North Star: Canadian Competitiveness in an Intangibles Economy. Public Policy Forum. *https://ppforum.ca/wp-content/uploads/2019/04/PPF-NewNorthStar-EN4.pdf.*

[13] Gartner. 2018. "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019." *https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.*

[14] Accenture. 2017. Exploring Next Generation Financial Services: The Big Data Revolution. *https://www.accenture.com/t20170314t051509__w__/nl-en/_acnmedia/pdf-20/accenture-next-generation-financial.pdf.*

COVID-19: LEVERAGING DATA IN A CRISIS

In 2019, a novel coronavirus (COVID-19) caused an outbreak of pneumonia in Wuhan, China before rapidly spreading across the globe. On March 11, 2020, the World Health Organization (WHO) officially declared COVID-19 a pandemic as governments distributed testing kits, closed public spaces, quarantined residents, and restricted travel to help contain the virus.

Throughout the crisis, regional and international health agencies have worked closely to track and analyze COVID-19. The volume of information shared across organizational and geographic boundaries has been unprecedented. Access to real-time data has enabled experts to make informed recommendations, while the public is able to stay up-to-date at a time when disinformation could be catastrophic.

Several tools were quickly deployed to synthesize data from multiple sources. In Canada, where health data is collected differently in each province, it became critical to standardize and aggregate data at the national level. On-going initiatives include #HowsMyFlattening, a centralized hub monitoring Ontario's response to COVID-19.[15] ThinkData Works, a Toronto-based data access company, has partnered with Roche to standardize and publish COVID-19 data from sources around the world.[16] The Canadian Institute for Health Information created a webpage with aggregated information about hospital beds, intensive care units, ventilators, the distribution of health-care workers, and more. [17]

Countless other examples include Nextstrain, a project focused on genome data, and the COVID-19 Open Research Dataset.[18] The supply and demand of these tools during the pandemic reflects the essential role data plays in managing a modern crisis.

Meanwhile, the Ontario government is working with industry and academic partners to develop a new Ontario Health Data Platform. At the time of writing, the intention is to give researchers access to anonymized data to help detect cases, predict locations of future outbreaks, and assess the effectiveness of containment measures. The platform is expected to integrate data from physician claims, medical drug claims, hospital discharge summaries, and several other sources.[19]

Finally, the pandemic has elevated a conversation about the ethical challenges of using personal data in innovative ways. This has been particularly evident in debates about contact tracing, as governments, public health agencies, and technology firms work together to develop cell phone applications that can notify individuals who may have come into contact with someone who has tested positive for COVID-19, all while preserving privacy. Various countries, including Singapore and Australia, have already introduced contact tracing apps. At the time of writing, Google and Apple are proposing a Bluetooth-based system with extensive measures to prevent re-identification of anonymized data.[20] In Ontario, applications under development include MyTrace (by the University of Toronto) and TraceScan (by the University of Waterloo and Facedrive).[21]

[15] #HowsMyFlattening. *https://howsmyflattening.ca/#/home.* Accessed April 15, 2020.

[16] ThinkData Works. 2020. "ThinkData Part of Roche Data Science Coalition to Fight COVID-19." *https://blog.thinkdataworks.com/press/thinkdata-works-covid-19-data-repository-press-release.*

[17] Canadian Institute for Health Information. 2020. "COVID-19 resources." *https://www.cihi.ca/en/covid-19-resources.*

[18] Nextstrain. "Genomic epidemiology of novel coronavirus." *https://nextstrain.org/ncov. Accessed March 20, 2020; and COVID-19*

[19] Open Research Dataset (CORD-19). 2020. *https://pages.semanticscholar.org/coronavirus-research.*

[20] Google. "Privacy-Preserving Contact Tracing." *https://www.apple.com/covid19/contacttracing/.* Accessed April 13, 2020.

[21] Paul Fraumeni. 2020. "U of T researcher aims to improve accuracy of COVID-19 contact tracing with MyTrace app." University of Toronto. *https://www.utoronto.ca/news/u-t-researcher-aims-improve-accuracy-covid-19-contact-tracing-mytrace-app*; and Financial Post. 2020. "Facedrive and the University of Waterloo Develop "TraceScan" App to Help Mitigate COVID-19 Spread." *https://business.financialpost.com/pmn/press-releases-pmn/business-wire-news-releases-pmn/facedrive-and-the-university-of-waterloo-develop-tracescan-app-to-help-mitigate-covid-19-spread.*

CHAPTER I ONTARIO'S DATA-DRIVEN ECONOMY

THE OPPORTUNITY

Data presents a clear opportunity for Ontario. When mobilized effectively, it can empower users to identify needs, evaluate solutions, improve productivity, catalyze innovation, and develop new areas of economic activity. Everything from climate change to labour shortages can be addressed more effectively with better data. The future looks especially promising for a province that has established itself as a leader in AI. [22]

Yet, along with its many benefits, the data revolution comes with potential risks, including the erosion of personal privacy and security, workforce disruption, market concentration, and increasing regional inequality. Governments around the world are reacting differently as they seek to balance the benefits and costs of a data-driven world. Ontario too needs to protect against these threats to build an environment in which data is a positive force for both individuals and businesses.

However, the need for caution should not negate the need to be proactive. The proliferation of digital and data-driven business models is part of a broader transition to an intangibles economy, where data and intellectual property (IP) are becoming more valuable than physical assets. In this new world, competitiveness is largely driven by the accumulation of data and networks that enable businesses to generate large returns at little or no marginal costs.[23]

As a result, Ontario's long-term competitiveness will depend on its ability to capitalize on the disruptive potential of data. Policymakers, in collaboration with businesses and other stakeholders, will need to foster the right regulatory frameworks, skillsets, and incentives.

The Governments of Canada and Ontario both recognize the significance of this transition. In May 2019, the federal government launched *Canada's Digital Charter*, a principles-based framework aimed at building a foundation of trust and unlocking Canada's innovation potential in the digital age.[24] The Government of Ontario is in the process of developing its own data strategy with a Digital and Data Task Force informed by industry consultations.[25] The following chapters outline recommendations to help build on these initiatives and firmly position Ontario for long-term success and global competitiveness within the data-driven economy.

[22] CPA Ontario. 2019. Evolving Alongside Artificial Intelligence. *https://media.cpaontario.ca/insights/ai/cpa-ontario-evolving-alongside-artificial-intelligence.pdf#1.*

[23] Asselin and Speer. 2019.

[24] Government of Canada. 2019a. Canada's Digital Charter in Action: A Plan by Canadians, for Canadians. *https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html.*

CHAPTER II

PRIVACY

A functioning data economy requires a solid foundation of trust between individuals and the organizations that collect, use, and share their personal information. As the uses of data have expanded, the public has grown increasingly wary of how their data is purposed and anxious about their personal privacy.

In a 2018 global survey, more than 50 percent of individuals said they had become more concerned about their online privacy compared to the previous year.[26] Another survey revealed that only 38 percent of Canadians agree that businesses respect their privacy rights.[27] In Ontario, a survey by the provincial government found that only 8 percent of respondents think businesses generally do a good job of explaining what they plan to do with consumers' data.[28]

Restoring trust will require collaboration among stakeholders. For businesses, the incentive is twofold. First, without public trust in the economy overall, companies will find it increasingly difficult to convince customers to use their products and services. Second, those that build trust through their own policies and practices, even at a short-term cost, will likely prove to be more competitive in the data-driven economy.[29]

Data governance frameworks should seek to protect individual privacy rights while encouraging innovation. While it can be challenging to navigate the trade-off between these two objectives, finding the right balance is fundamental to a successful modern economy.

[25] Government of Ontario. "Ontario's Digital Strategy." *https://www.ontario.ca/page/ontarios-data-strategy.* Accessed April 30, 2020.

[26] Umberto Bacchi. 2019. "Factbox: Hacks and facts - 10 things you didn't know about data privacy." Reuters. *https://www.reuters.com/article/uk-global-tech-privacy-factbox/factbox-hacks-and-facts-10-things-you-didnt-know-about-data-privacy-idUSKCN1PM29H.*

[27] OPC. 2019. "2018-19 Survey of Canadians on Privacy." *https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/.*

[28] Government of Ontario. "Ontario's Digital Strategy." *https://www.ontario.ca/page/ontarios-data-strategy.* Accessed April 30, 2020.

[29] Mastercard. 2019.

CHAPTER II PRIVACY

PRIVACY IN ONTARIO: WHICH RULES APPLY?

In Ontario, different organizations are subject to different privacy frameworks (see Table 1). The Office of the Privacy Commissioner of Canada (OPC) and the Information and Privacy Commissioner of Ontario (IPC) are each responsible for investigating privacy complaints related to their respective jurisdictions, commenting on proposed government policies, and informing stakeholders about privacy laws.

The OPC and the IPC provide valuable guidance to organizations on issues ranging from general to specific. For example, the OPC has material on e-marketing, consent, and cannabis transactions. The IPC's library includes guidance on video surveillance, privacy in school, and de-identification techniques.

TABLE 1: PRIVACY AUTHORITIES FOR ORGANIZATIONS IN ONTARIO

REGULATED ENTITIES	PRIVACY FRAMEWORK	OVERSIGHT AGENCY
Businesses and others engaging in commercial activity	Personal Information Protection and Electronic Documents Act (PIPEDA)	OPC
Federal departments and agencies	Privacy Act	OPC
Provincial departments and agencies	Freedom of Information and Protection of Privacy Act (FIPPA)	IPC
Municipal departments and agencies	Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)	IPC
Health information custodians	Personal Health Information Protection Act (PHIPA)	IPC

Regional governments may be tempted to introduce additional rules as the general public grows more concerned about privacy. The United States finds itself moving in this direction with California's recent implementation of the California Consumer Privacy Act. Three Canadian provinces (Alberta, British Columbia, and Quebec) also have their own private-sector privacy laws, though these are deemed substantially similar to PIPEDA and are applied in its place.

This trend towards fragmentation is concerning. By and large, the existing division of responsibilities between federal and provincial authorities has worked well. Stakeholders understand which rules apply to them and to whom they are accountable. A patchwork of privacy rules would complicate the business environment and act as an unnecessary interprovincial trade barrier. While it may make sense for provincial and local governments to develop data strategies to improve their internal uses of data and broadly support their local digital economies, they should refrain from creating a patchwork of policies and programs.

POLICY RECOMMENDATION

The Government of Ontario should avoid duplicating federal government laws pertaining to the collection, use, and disclosure of personal information by private sector organizations.

CHAPTER II PRIVACY

MODERNIZING PRIVACY (PHIPA AND PIPEDA)

Most national privacy laws were written decades ago, when data uses were far less sophisticated than they are today. With a trend towards more data collection, many communities are questioning the adequacy of those regimes and amending them with the intention of preserving democracy and individual rights. The European Union (EU) and California are two examples of jurisdictions that recently introduced new privacy laws. In 2019, the Government of Canada announced its intention to modernize PIPEDA, the *Privacy Act*, the *Competition Act*, and the *Statistics Act*.

PIPEDA and PHIPA are widely regarded as being robust, principles-based privacy frameworks. There is some debate within Canada about whether it makes sense to move towards the more prescriptive approach taken by the GDPR. This approach has its merits in the EU, where it has created a single standard across very different countries, forced organizations to take a closer look at their privacy practices, and increased the general public's data literacy.

However, highly prescriptive rules around how organizations can collect, process, and share data make it more difficult to use data in valuable new ways as technology progresses. The GDPR assumes that a one-size-fits-all approach to privacy makes sense for all sectors, and that the chosen rules will stand the test of time. Implementation of the framework has also come at a high cost. Some estimates suggest the first year of GDPR led to a decline in venture funding and the creation of more than 100,000 compliance jobs.[30] High compliance burdens make it more difficult for smaller firms to compete with larger ones.[31] Further, a focus on compliance can result in a convergence around minimum obligations, while an effective data-driven economy should encourage data custodians to do the most they can to win over public trust.

UPDATED PRIVACY FRAMEWORKS IN EUROPE AND CALIFORNIA

EUROPE: THE GENERAL DATA PROTECTION REGULATION

Effective 2018, the General Data Protection Regulation (GDPR) governs the collection and processing of personal information of individuals who live in the EU. Key features of the GDPR that differ from PIPEDA include:

- Individuals' right to data portability;
- The principle of privacy by design; and
- Clearer, stronger enforcement powers and administrative monetary penalties.

The GDPR requires comparable data protection legislation in regions where personal data is transferred as a prerequisite for international data transfers. The EU has recognized Canada's federal privacy laws as providing adequate protection to its own laws, but this adequacy status is set to come under review no later than 2020.

CALIFORNIA: THE CALIFORNIA CONSUMER PRIVACY ACT

The California Consumer Privacy Act (CCPA) came into effect on January 1, 2020. Unlike the GDPR, it only applies to for-profit entities that meet a size threshold (i.e. have gross annual revenues of at least $25 million USD; handle the personal information of 50,000 or more consumers, households, or devices; or derive 50 percent or more of annual revenues from selling consumers' personal information).

The CCPA is designed to enable consumers in California to know what personal information businesses are collecting from them, require businesses to delete that information, and opt out of the sale of their data to third parties. Companies that intentionally violate the CCPA can face fines of up to $7,500 USD per violation.

[30] Robert Atkinson. 2019. "Regent Debate: Beware of Overeager Regulation." C.D. Howe Institute. *https://www.cdhowe.org/intelligence-memos/robert-atkinson-regent-debate-beware-overeager-regulation.*

[31] Royal Bank of Canada (RBC). 2020. "RBC Disruptors - Is Data Bigger than Oil?" (Podcast). *https://soundcloud.com/rbcdisruptors/is-data-bigger-than-oil.*

CHAPTER II PRIVACY

Protecting privacy is imperative. Canada's existing principles-based frameworks provide a foundation for achieving this goal. As further regulatory advances are made, the objective should be to retain legislative flexibility that allows for innovation while pushing organizations to implement and maintain robust privacy practices.

This can be done in large part by strengthening **industry standards** or **codes of practice**.[32] Standards outline specific practices organizations should follow to achieve their legal obligations. Unlike legislation, standards can be updated quickly and frequently to adapt to changing realities in the data-driven economy, and sector-specific standards have the added benefit of being relevant to the unique challenges of different industries. Additionally, they can be developed into certification programs, which provide a helpful signal to consumers.

The National Standard of Canada (NSC)'s Model Code for the Protection of Personal Information (CAN/CSA-Q830-96) is considered an integral part of PIPEDA, but it was developed in 1996 and may not contain enough detail to address modern uses of data.

To that end, the Chief Information Officers (CIO) Strategy Council of Canada is undertaking a series of projects to define data privacy standards around the collection, maintenance, sharing, and use of big data in different sectors of the economy.[33] Other ongoing initiatives are more sector-specific. The Government of Canada recognizes the importance of developing and promoting data governance standards and has indicated they will play an important role in Canada's digital economy.[34]

There is ample room for more widespread recognition and adoption of industry standards, and a need to define stronger ones where they do not exist. Businesses should contribute to their development and adopt those that are relevant to their fields. Standards should be reviewed and updated regularly to address the rapidly evolving challenges around data privacy, many of which are discussed below.

Although codes are voluntary, they can become so widely accepted that they are seen as effectively mandatory. Governments should also consider updating PIPEDA and PHIPA to refer explicitly to the existence of standards, and in some situations recommend organizations adopt industry standards as a means to demonstrate compliance with privacy laws. The OPC and the IPC could choose to publish lists of recognized standards on their websites. In any case, it is important for specific data governance standards to remain outside legislation, as this allows them to be updated easily and regularly.

POLICY RECOMMENDATION

The Governments of Canada and Ontario should preserve the principles-based nature of PIPEDA and PHIPA while encouraging the development and widespread adoption of industry standards or codes of practice.

BEST PRACTICE

Organizations should collaborate on an ongoing basis to develop and adopt privacy standards that enhance public trust in their respective sectors.

[32] Note: Industry standards and codes of practice are used interchangeably in this report.

[33] CIO Standards Council of Canada. "Notice of Intent." *https://ciostrategycouncil.com/standards/new-projects/.* Accessed April 4, 2020.

[34] Government of Canada. 2019a.

CONSENT

At the heart of PHIPA and PIPEDA is a requirement that regulated entities obtain consent from individuals when collecting, using, or sharing their personal information. In certain cases, these frameworks also allow organizations to obtain *implied* consent when using data in ways that individuals should reasonably expect.

Obtaining consent has become more challenging over time as personal information is collected through new tools, including facial recognition software, wearable technologies, and smart home devices. Further, most consumers are inundated with so many terms and conditions that it becomes difficult to ensure their consent is informed and meaningful.

Organizations should ensure consent is obtained in a meaningful manner. Best practices include:

- Phrasing consent notices in terms that can be understood at a grade seven or other appropriate level of comprehension.
- Applying lessons from behavioural insights to design terms and conditions such that consumers better understand what they are consenting to. For example, it helps to provide information in shorter pieces at relevant times.[35]
- Offering consumers different options for consent, which could involve proportional tiers of service and/or pricing.
- Continuously updating consent policies as technologies and consumer literacy evolve.

BEST PRACTICE

Organizations should structure consent policies conscientiously to ensure customers are meaningfully informed of their options and empowered to exercise those options.

There is also a need for more clarity around when explicit consent is necessary and how organizations are expected to obtain meaningful consent under different scenarios. A specific question for many sectors is the extent to which explicit consent is necessary when sharing de-identified information. As will be discussed in Chapter V, the health care sector would benefit from a consistent interpretation of the conditions under which personal health information can be shared with third parties.

In many cases, official guidance and industry standards could help clarify best practices within different sectors or for specific industry activities, where considerations may vary. More broadly, the Business Council of Canada has recommended amending PIPEDA to clarify that a business can use personal information without explicit consent when doing so is necessary to meet legal obligations, protect an individual's vital interests, promote the public interest, or support a legitimate interest or standard business practice. [36]

POLICY RECOMMENDATION

The Governments of Ontario and Canada should facilitate the development of clear expectations around consent through a combination of legislative amendments to PHIPA and PIPEDA, clear guidance, and industry standards.

[35] The Behavioural Insights Team. 2019. Best practice guide: Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses. *https://www.bi.team/wp-content/uploads/2019/07/BIT_WEBCOMMERCE_GUIDE_DIGITAL.pdf.*

[36] Business Council of Canada. 2020. Data Driven: Canada's Economic Opportunity. *https://thebusinesscouncil.ca/wp-content/uploads/2020/02/Data-Driven-Report.pdf.*

DATA LOCALIZATION

Data localization legally requires organizations to store and process data within domestic borders, often to protect privacy, national security, or economic nationalism.[37] Localization requirements can vary in their strictness. Some countries, including China, Turkey, and Australia, require it for specific industries or categories of data. Others, including EU members subject to the GDRP, require companies to ensure there is a minimum level of data protection in the jurisdictions where they store data, and/or to obtain consent from customers before transferring their personal information abroad.

Neither PIPEDA nor PHIPA currently require localization, though both hold organizations accountable for data that is transferred outside Canadian borders by applying the same privacy obligations. Additionally, organizations need to notify individuals if their information may be processed in a foreign country and inform them that it may be accessible to law enforcement and national security authorities of that jurisdiction.[38]

There is disagreement within Canada as to whether some degree of legal restrictions on data transfers are appropriate. Strict data localization is particularly onerous for organizations that rely on international data transfers for business functions such as human resources, legal, and shipping. [39] Localization can also prevent local firms from accessing global datasets needed to power AI and other advanced data analytics. This is a big challenge for AI firms located in Canada, where a small population often makes it necessary to access foreign data to build robust AI models.

That said, protecting the privacy and security of data transferred abroad is critical. Trade agreements offer one avenue for this. While these documents often include clauses that prohibit strict localization, they simultaneously require countries to implement minimum privacy standards, enter into cooperation agreements for data security and law enforcement, and/or use other mechanisms to mitigate the risks of cross-border data transfers. Sector-specific agreements can also serve this purpose.

Alternatively, the GDPR requires other countries to have an "adequate level of data protection" in order to receive EU citizens' data.[40] Given the EU's market size, this provision will likely incentivize foreign governments to strengthen their internal frameworks, and Canada will benefit as a result.

POLICY RECOMMENDATION

The Governments of Canada and Ontario should build on international efforts to secure interoperability of privacy standards and ensure that Canadian authorities have immediate and complete access to information stored abroad for the purposes of investigation and enforcement.

BEST PRACTICE

Organizations should exercise due diligence to ensure they are able to meet their privacy and security requirements when transferring information to other jurisdictions.

[37] Institute of International Finance. 2019. Data Flows Across Borders: Overcoming Data Localization Restrictions. *https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf.*

[38] OPC. 2014. "Privacy and outsourcing for businesses." *https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/outsourcing/02_05_d_57_os_01/.*

[39] Business Council of Canada. 2020.

[40] European Commission. "Adequacy decisions." *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.* Accessed April 30, 2020.

DATA PORTABILITY

Most privacy frameworks – including PIPEDA and PHIPA – allow individuals to access their personal information held by businesses, challenge its accuracy, and have it corrected. A more contentious question is whether people should have the right to have their data transferred from the organizations that collect it to third parties in a common, machine-readable format (a practice known as data portability).

The United Kingdom, the EU, and Australia have given individuals the right to data portability in different ways. *Canada's Digital Charter* recognizes the value of data portability, noting that it can benefit Canadians by fueling choice and competition.[41]

However, data portability means different things for different industries. In some sectors, the benefits are clear and there is good reason to move forward with consumers' right to data portability. In other cases, the benefits are less clear and there may be unique risks to consider around privacy and identity thefts, or the potential unintended consequences of deterring innovation by requiring businesses to share data with competitors.

An industry-by-industry approach allows organizations within each sector to work together, along with government, to define common privacy and security standards around data access and portability. Each industry will have unique legacy systems and considerations that need to be addressed.

Again, this is an opportunity to develop stronger codes of practice. Where there is a clear benefit to consumers, governments should work with industry to develop codes related to access and portability. In cases where the benefits to consumers are minimal, or the risks to organizations are significant, it makes sense to proceed more cautiously.

Open banking is one manifestation of the data portability principle and Canada has done well to take a measured approach thus far. Meanwhile, policymakers should evaluate the effectiveness of portability policies in other jurisdictions to inform their approaches.

Further, it is important to distinguish between personal data and information that an organization has collected, combined with other sources, and generated (known as imputed data). When companies use their own resources to apply insights to personal data, the new information they create becomes IP, often critical to their competitive advantage. Australia has excluded imputed data, as well as data that cannot be re-identified, from portability requirements.

POLICY RECOMMENDATION

The Government of Canada should take a measured, industry-specific approach to data portability and allow sufficient time for businesses to implement any new requirements.

BEST PRACTICE

Organizations should facilitate data portability where doing so could have material benefits for consumers without unreasonably increasing risk.

[41] Government of Canada. 2019a.

CHAPTER II PRIVACY

PRIVACY BY DESIGN

The principle of privacy by design requires organizations to give data protection due consideration at all stages when developing their systems, software, solutions, and services. The concept originated in the 1990s by Ontario's former Information and Privacy Commissioner, Dr. Ann Cavoukian.[42]

PIPEDA and PHIPA do not explicitly require privacy by design, though it could be seen as an implicit requirement for organizations to meet their other obligations under these frameworks. Practical guidance from privacy commissioner offices, industry regulators, and/or standard-setting bodies can help organizations better operationalize this principle.

Guidance around de-identification techniques is particularly helpful to those adopting privacy by design. For example, one technique more organizations could adopt is known as differential privacy, which involves adding random noise to datasets to prevent them from being de-anonymized.[43] Differential privacy has been increasingly adopted by businesses, as well as the US Census Bureau, in response to evidence that individuals can be identified from allegedly anonymized datasets when multiple sources are combined.[44]

Another best practice related to privacy by design is data minimization, the notion that organizations should minimize the amount of personal information they collect. While guidance does exist around these practices, there is room for more organizations to include them within their privacy policies.

POLICY RECOMMENDATION

The Governments of Ontario and Canada should continue promoting privacy by design as a best practice to help organizations comply with PIPEDA and PHIPA.

BEST PRACTICE

Organizations should incorporate privacy by design across their systems, where feasible, and keep up with the most up-to-date guidance and standards as they evolve.

PRIVACY IMPLICATIONS OF COVID-19 CONTACT TRACING

As noted in Chapter I, governments around the world are adopting contact tracing technologies to help identify and notify individuals who may have come into contact with people who have tested positive for COVID-19. These digital solutions can potentially complement other efforts by governments to track and contain the outbreak; however, they also raise questions around privacy and data protection.

The contact tracing technologies being adopted have varying degree of privacy by design embedded within them.[45] For example, many of the apps do not collect location data or other identifiable information but instead generate temporary encrypted IDs and rely on Bluetooth to identify other phones in a user's proximity. Many apps are also designed to only hold data for thirty days or less, and governments may choose to legally limit who can access the data and for what purpose.

In April 2020, the OPC published a framework to assist government institutions preserve privacy as they respond to COVID-19.[46] It includes considerations around de-identification, purpose limitation, transparency, time limitation, and other key privacy principles. In the context of contact tracing, the framework points out that location data can be very challenging to fully anonymize and the risk of re-identification needs to be considered.

Overall, differences in design and governance will ultimately determine whether an innovative use of data collection is both legal and ethical. Privacy by design helps ensure that new technologies have appropriate measures in place to maximize privacy and data security.

[42] IPC. 2013. Privacy by Design. *https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf.*

[43] Michael Kearns and Aaron Roth. 2020. "Ethical Algorithm Design Should Guide Technology Regulation." The Brookings Institute. *https://www.brookings.edu/research/ethical-algorithm-design-should-guide-technology-regulation/.*

[44] Ibid.

[45] OECD. 2020. "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics." *https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics/.*

[46] OPC. 2020. A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19. *https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/.*

ACCOUNTABILITY

To protect health care data privacy, the IPC has the power to impose orders on organizations found to be violating obligations under PHIPA. In March 2020, maximum penalties for violating PHIPA were doubled and the IPC was given the power to levy monetary penalties directly.

However, weaker enforcement mechanisms apply to commercial privacy law under PIPEDA, which many critics say lacks teeth.[47] Under the GDPR, European data authorities can impose fines worth 4 percent of worldwide revenue or 20 million euros, whichever is greater, and order companies to erase data or stop processing it. By contrast, the OPC does not have order-making powers. It can only enter into voluntary compliance agreements or refer cases to the courts for prosecution.

In its *Digital Charter*, the Government of Canada acknowledges the need for strong enforcement mechanisms and commits to examining options to strengthen the OPC's powers.[48] However, stakeholders disagree about the extent to which the OPC's enforcement powers should be expanded. The OPC and others in favour of empowering the agency to directly order companies to comply with the law and impose penalties for non-compliance say this is necessary to restore public trust, create a clear incentive for good behaviour, and maintain Canada's adequacy under the GDPR.[49]

Others argue there is no compelling evidence that the current enforcement regime is insufficient. In the few cases where parties were unable to reach a resolution, Section 15 of PIPEDA allows the OPC to bring the case to the Federal Court, which has significant powers to levy penalties. There is a concern that giving the OPC greater enforcement powers could compromise the office's ombudsman role, making organizations uncomfortable approaching the OPC for information and guidance when they are contemplating using data in new ways.

As a middle ground, the Business Council of Canada recommends giving the OPC new tools, such as limited order-making powers in certain cases, including where there is a risk of material harm to individuals, while giving the courts more tools to impose fines for serious cases of non-compliance.[50]

On balance, greater enforcement may be necessary, but the focus should be on where there are real risks to individuals. As discussed above, it may make sense in some cases for industry regulators to take on a greater enforcement role where there are established standards.

POLICY RECOMMENDATION

The Government of Canada should take measured steps to strengthen enforcement of privacy laws, which may include giving the OPC limited order-making powers, while preserving the current ombudsman model.

Transparency also helps strengthen accountability. Only 43 percent of organizations responding to the OCC's 2020 Business Confidence Survey said they had data policies.[51] As a first step, all businesses should make it easy for anyone to understand the conditions under which they will collect, store, and use data assets. Privacy disclosures should be more comprehensive than most currently are, including information about any significant uses of personal information for AI purposes.[52]

While not a complete solution, transparency can help both consumers and regulators identify potential areas of concern. It helps establish a competitive market where consumers can make informed decisions and vote with their dollars, and civil society can respond by developing platforms and resources to help the public compare privacy practices.

Within the health sector, effective transparency entails more than providing information about how data is used, but also involving the public in the decision-making process to the extent this is feasible.[53] Health care organizations in the United Kingdom are generally seen as good examples when it comes to transparency.

BEST PRACTICE

Organizations should embrace transparency by openly communicating details about their data privacy practices.

[47] For example, see: Teresa Scassa. 2020. "How Facebook's Poor Privacy Practices Shed Light on PIPEDA's Shortcomings." Centre for International Governance Innovation. *https://www.cigionline.org/articles/how-facebooks-poor-privacy-practices-shed-light-pipedas-shortcomings.*

[48] Government of Canada. 2019a.

[49] OPC. 2019. "2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act." *https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/.*

[50] Business Council of Canada. 2020.

[51] A survey of n=1240 OCC members was conducted online by Golfdale Consulting between October 2 and November 10, 2019.

[52] Cameron F. Kerry. 2020. "Protecting privacy in an AI-driven world." The Brookings Institute. *https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/.*

[53] Ashley Challinor. 2017. Driving Digital Innovation in the Ontario Health Care System. OCC. *https://occ.ca/wp-content/uploads/Driving-Innovation-Dec-7-1.pdf.*

CHAPTER II PRIVACY

GOVERNMENT DATA

Governments, like businesses, collect valuable information, including census data, tax returns, transit patterns, and administrative data. In the context of smart city applications and digital government solutions, the amount of data in the hands of governments has grown exponentially. Consequently, the privacy policies they apply to that data are no less important than those of other organizations.

Civic data trusts are one governance model to consider in the context of smart cities. These are contracted entities established to manage data that could be considered a public asset, where independent trustees are given the authority to make decisions around data ownership, collection, security, rights, and usage. Several civic data trust pilot projects are already underway in the United Kingdom.[54]

Data trusts could help governments unlock data-driven innovation while remaining accountable to the public. The model is relatively new, and will require thoughtful development of appropriate legal structures, funding, and incentives. Starting with smaller, more limited applications of the model can help stakeholders evaluate its merits and limitations before deciding if and how to scale.

POLICY RECOMMENDATION

Ontario's provincial and municipal governments should experiment with small-scale civic data trusts.

[54] Asselin and Speer. 2019.

CASE STUDY: DATA FOR GOOD BY TELUS

TELUS has long recognized the value of using data to achieve social good. During the COVID-19 pandemic, the Canadian telecommunications and health care technology company put this commitment into action by launching a new initiative called Data for Good.[55]

The Data for Good program provides governments, health authorities, academic researchers, and other stakeholders with access to de-identified network mobility data and insights to help them respond more effectively to COVID-19. By giving stakeholders free access to its TELUS Insights service, TELUS is supporting a variety of efforts to stem the spread of the virus, lessen impacts on health and the economy, coordinate health care responses, and carry out research that could mitigate or prevent future phases of COVID-19 or future pandemics.

For example, data scientists can analyze network mobility data from TELUS in conjunction with case counts of COVID-19 in different regions to help governments develop public policy responses and decide where to allocate limited resources. Similarly, data showing the number of people visiting certain locations can help research and academic institutions assess the economic impacts of COVID-19.

Data for Good is a privacy-first program, reflecting TELUS' long-standing commitment to using data responsibly. The TELUS Trust Model, which centres around the core principles of accountability, ethical use, and transparency guides all data-driven practices across the business.[56] TELUS worked with privacy and technology experts to develop models that allow insights to be derived from network mobility data without compromising individuals' privacy. The result is that when data is shared with third parties, it is strongly de-identified and aggregated in accordance with leading industry standards to ensure privacy is fully protected at all times without compromising the utility of the data and the insights it provides.

With a robust data governance framework in place, TELUS was able to develop and launch Data for Good swiftly as the need for network mobility data became apparent earlier this year. The program is run by the TELUS Data & Trust Office and powered by TELUS Insights, a data analytics practice that has received Privacy by Design certification.[57] To further protect privacy, stakeholders are required to limit their use of the insights and datasets to the ethical purposes outlined on the TELUS website.[58]

TELUS remains committed to leveraging de-identified network mobility data for a variety of public purposes beyond COVID-19. The TELUS Insights service helps government agencies, non-profits, and other organizations make more informed and strategic decisions.[59] For communities, it contributes to emergency response, improved health outcomes, and better public services. For customers, this leads to best-in-class services, optimized reliability, and superior customer experiences. As opportunities to use data to improve the lives of Canadians increase, TELUS will continue to build trust with stakeholders by using data in a way that generates value, promotes respect, and delivers security.

[55] TELUS. "Data for Good: Leveraging TELUS data against COVID-19." *https://www.telus.com/en/about/covid-19-updates/privacy-statement.* Accessed June 1, 2020.

[56] TELUS. 2019. "The TELUS Trust Model." *https://www.telus.com/en/about/privacy/trust-model.*

[57] Professional Evaluation and Certification Board. "Certifications Granted." *https://pecb-ms.com/en/certifications-granted.* Accessed June 1, 2020.

[58] TELUS. "Data for Good: Leveraging TELUS data against COVID-19."

[59] TELUS. "TELUS Insights." *https://www.telus.com/en/on/business/medium-large/enterprise-solutions/big-data-analytics.* Accessed June 1, 2020.

CHAPTER III

CYBERSECURITY

While robust privacy rights are necessary to protect sensitive information, it is equally important to safeguard that data against unauthorized access and use. Over time, the field of data security has grown increasingly complex as more information is stored electronically. Today's cybercriminals are sophisticated and agile, using a variety of techniques to illegally obtain data from individuals and organizations of all sizes.

According to a 2018 survey of Canadian businesses, 40 percent of respondents experienced a cyber attack in the previous twelve months.[60] The average cost to companies is estimated to be $5 million.[61] This challenge is only expected to grow, in part because the attack surface is growing as more devices, sensors, and autonomous vehicles connect to the Internet. Juniper Research estimates that cybercriminals will obtain more than 33 billion records in 2023, an increase of 175 percent from 2018.[62]

Data breaches affect businesses of all sizes, in all sectors. Cybersecurity has a direct impact on individual and national security, business operations, the stability of critical infrastructure, and public trust. The COVID-19 pandemic has increased the risk, as many interactions have shifted online through an expanded use of telecommuting, e-commerce, virtual care, and other digital services. Cybercriminals have also taken advantage of people's heightened levels of concern and fear around COVID-19, with malware and phishing emails designed to scam people out of their money or personal data.[63]

[60] Canadian Internet Registration Authority. 2019. "2018 Cybersecurity survey report." *https://cira.ca/resources/cybersecurity/report/2018-cybersecurity-survey-report.*

[61] IBM. 2019. 2019 Cost of a Data Breach Report. *https://www.ibm.com/security/data-breach.*

[62] Juniper Research. 2019. The Future of Cybercrime & Security. *https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security.*

[63] Canadian Centre for Cyber Security. 2020. "Staying cyber-healthy during COVID-19 isolation." *https://cyber.gc.ca/en/news/staying-cyber-healthy-during-covid-19-isolation.*

PREVENTING BREACHES

Organizations subject to PIPEDA and PHIPA are legally required to protect sensitive information in their possession against loss or unauthorized access. PIPEDA, for example, specifies that, "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."[64]

Organizations are also required to report certain categories of data breaches to their respective privacy commissioner and any affected individuals. In the case of PIPEDA, this includes any breach that poses a real risk of significant harm to individuals. The OPC and the IPC may then investigate whether affected organizations had taken appropriate measures to safeguard their systems and recommend remedial measures if appropriate. Mandatory breach requirements were introduced under PIPEDA in 2018 and strengthened under PHIPA in 2019. They form an essential feature of any strong data governance framework, a necessary tool to remedy security gaps and protect individuals.

In general, most organizations' cybersecurity budgets are relatively low and too few are adequately assessing their cyber risks.[65] The OCC's 2020 Business Confidence Survey found organizations in Ontario have very different levels of cybersecurity. Nearly half (49 percent) of the respondents said their organizations had trained employees on data security and/or privacy, and 23 percent said their organizations had cybersecurity insurance. Others reported measures included installing firewalls, introducing multi-factor authentication, moving data to the cloud, and outsourcing security systems.[66]

Unfortunately, there is no bulletproof solution. Ideally, cybersecurity should be thought of as not just an IT issue but a broader society-wide challenge that requires ongoing collaboration. Risks should be regularly assessed, systems continually upgraded, and data security embedded into all procedures and systems at the outset.

Industry standards can go a long way in improving overall security postures. Standards help organizations understand what is expected of them from a cybersecurity perspective while certifications signal a minimum level of protection to regulators and the public. Specific techniques should not be prescribed within legislation, since flexibility is essential to ensure standards remain relevant as risks and technologies evolve.

[64] PIPEDA, SC 2000, c. 5.

[65] EY Canada. 2019. Cybersecurity: Do you know which protective measures will make your company cyber resilient? *http://www.chamber.ca/events/ey_21st_global_information_security_survey_2018_2019.pdf.*

[66] A survey of n=1240 OCC members was conducted online by Golfdale Consulting between October 2 and November 10, 2019.

CHAPTER III CYBERSECURITY

Public and private sector organizations should adopt globally recognized standards where possible. These include the International Organization for Standardization (ISO) 27001, ISO 27017, and ISO 27018; the American Institute of Chartered Professional Accountants (AICPA) System and Organization Controls (SOC) 2 and AICPA SOC 3; the US Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1; and the Information Security Forum (ISF) Standard of Good Practice for Information Security.

The CIO Strategy Council of Canada is also developing industry standards around data security and secure digital identities.[67] Security considerations can vary somewhat by sector; for instance, Ontario's health care providers may benefit from guidance on communicating via fax machine, which remains a common practice within that sector.

Smaller businesses also have unique advantages and disadvantages when it comes to cybersecurity, generally being less resourced but nimbler. The Government of Canada offers guidance with its *Get Cyber Safe Guide for Small and Medium Businesses*, as well as a certification program called CyberSecure Canada, which promotes simple, low-cost baseline security controls.

The OPC has indicated in the past that organizations will be considered responsible for meeting industry standards or codes of practice where they do exist. This is the right approach, and one the federal and provincial governments could consider formalizing by referring to the existence of those standards explicitly within PIPEDA and PHIPA and/or by publishing a list of recognized standards.

POLICY RECOMMENDATIONS

The Governments of Ontario and Canada should adopt globally recognized cybersecurity standards internally and within the broader public sector.

The Governments of Ontario and Canada should encourage and monitor adoption of cybersecurity standards in sectors where they are not already enforced by regulators.

BEST PRACTICE

Organizations should adopt and maintain best-in-class cybersecurity standards.

[67] CIO Standards Council of Canada. 2020.

BUILDING CAPACITY

Ultimately, security standards are only helpful if organizations have the capacity to implement them. The Government of Canada has recognized this need, allocating more than $500 million in Budget 2018 towards the implementation of a National Cyber Security Strategy and the establishment of the Canadian Centre for Cyber Security, an institute focused on sharing information and deploying specialized cyber defence solutions.

Several other public-private initiatives also exist with a focus on capacity-building. In Ontario, these include the Rogers Cybersecure Catalyst at Ryerson University, the Cybersecurity Fintech Innovation Pilot Program, and the Waterloo Cybersecurity and Privacy Institute. Several efforts exist at the international level, including the Organization for Economic Cooperation and Development (OECD)'s Global Forum on Digital Security for Prosperity and the International Cyber Security Protection Alliance.

Other initiatives are sector-specific. For example, in 2019, ORION's Cybersecurity Higher Education Consortium established a framework for managing cybersecurity risks within Ontario's higher education sector.[68] The retail industry is also working together to share best practices and improve the sector's resiliency.

Sharing information about both threats and solutions is essential. The Canadian Cyber Threat Exchange (CCTX) was established for this purpose and allows member organizations to share information anonymously. Organizations should be encouraged to communicate with others in their sector about their experiences to disseminate learnings. Open dialogue is more productive than shaming, which can incentivize organizations to hide breaches. Where possible, this communication should cross provincial and international borders to reflect the multi-jurisdictional nature of cybersecurity threats.

Having a detailed understanding of the security landscape is necessary to determine where to allocate resources. It is important to consistently review whether there are specific sectors, regions, or types of organizations that are seeing more breaches than expected, and whether there are barriers to accessing existing government supports.

POLICY RECOMMENDATION

The Governments of Ontario and Canada should work with industry groups to assess the strengths and weaknesses of cybersecurity defences across the economy and, where appropriate, help to address them.

BEST PRACTICE

Organizations should share learnings and best practices to strengthen overall cybersecurity capacity within their sectors and the wider economy.

[68] ORION. "Ontario Cybersecurity Higher Education Consortium (ON-CHEC)." *https://www.orion.on.ca/about-us/on-chec/.*

For many organizations, one of the main barriers is a lack of expertise. There is a shortage for cybersecurity skills globally, and the competition for talent is especially challenging for smaller businesses and local governments. Collaboration between the public and private sectors is important to address this skills shortage and help Ontario retain the cybersecurity experts trained within the province. This partnership approach has been used successfully for skilled trades.

Ontario's public education system can also take steps to prepare future generations of workers. The province's Ministry of Education recently introduced a renewed curriculum with a stronger focus on math, STEM, and financial literacy. These changes should embed data and digital literacy at different stages in K-12 classes.[69]

POLICY RECOMMENDATIONS

The Government of Ontario should establish public-private partnerships focused on developing Ontario's cybersecurity talent pool and encouraging talent to remain in the province.

The Government of Ontario should continue to build pathways to data and digital literacy within the public education curriculum.

BEST PRACTICES

Key areas of focus for organizations looking to strengthen their cybersecurity postures include risk assessments, staff training, technology, and insurance.

RISK ASSESSMENTS

A first step for any organization is to understand its exposure to different threats, including any risks it absorbs indirectly, to inform appropriate fixes. For example, companies with complex supply chains should understand that they are only as strong as their weakest link. These firms may benefit from reviewing their contracts with suppliers to ensure they include right-to-audit clauses or they may consider applying blockchain technology to their interactions. Similarly, financial service providers might consider looking into the cybersecurity exposure of the businesses they lend to, in addition to the credit checks they already perform. Overall, cybersecurity is a strategic risk that executives and board members should be thinking about, instead of being solely considered within an organization's information technology (IT) department.

BEST PRACTICE

Organizations should carry out comprehensive cybersecurity risk assessments and regard cybersecurity as a business risk rather than an IT risk

[69] Deloitte Canada. 2020. Canada's most undervalued resource: The importance of capitalizing on the data economy. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-the-new-economy-data-report-aoda.pdf?icid=banner_download_btn.

CHAPTER III CYBERSECURITY

STAFF TRAINING

Since the biggest risk factor for data breaches is human error or negligence, educating staff about cyber hygiene is critical for any organization.[70] In a 2019 survey of Canadian employees, only 40 percent of respondents had received cybersecurity training at work, and the majority of those were trained once a year or less frequently.[71] Of those who did receive training, 93 percent said it had helped them mitigate threats.[72] Similar results were found in a study of Canadian health care professionals.[73]

A lack of employee training can undermine even the best defence techniques. For example, multi-factor authentication is widely regarded as a best practice, but busy staff may try to get around the practice if they do not properly understand its importance.[74] Training should be done regularly and include information about safely transferring digital files, who to alert after noticing a potential security incident, using social media wisely, and avoiding malware. [75]

BEST PRACTICE

Organizations should train staff regularly to build internal cyber hygiene.

TECHNOLOGY

Technology options to reduce cyber risk include AI tools that help organizations detect unauthorized access immediately and biometric devices, which achieve authentication using human characteristics such as fingerprints, facial recognition, typing rhythm, and voice. These solutions are available and growing in popularity.

Cloud infrastructure is another helpful option for most organizations. When configured well, data stored in the cloud can be more secure that data stored locally because reputable cloud service providers tend to have well-resourced security frameworks. However, reliance on the cloud can provide some organizations with a false sense of security and cause them to limit their own security measures. Legally, businesses are still responsible for the personal information they transfer to a cloud provider or other third party. Thus, when using cloud services, businesses should also monitor their own security strategies and retain sufficient internal expertise.[76] Further, since not all cloud vendors are created equal, data custodians should always look for those with appropriate capabilities to patch emerging vulnerabilities. Selecting the right provider will only become more important because cybercriminals are increasingly targeting cloud environments.[77]

BEST PRACTICE

Where appropriate, organizations should adopt technology to help staff manage cyber threats.

[70] Accenture. Cyber Threatscape Report. 2019. *https://www.accenture.com/_acnmedia/PDF-107/Accenture-security-cyber.pdf#zoom=50.*

[71] Scalar. 2019. The Digital Citizen: A Canada-wide Survey on Security Awareness in the Workplace.

[72] Ibid.

[73] Kaspersky. 2019. Cyber Pulse: The State of Cybersecurity in Healthcare – Part Two. *https://media.kasperskydaily.com/wp-content/uploads/sites/85/2019/08/16121510/Kaspersky-Cyber-Pulse-Report-2019_FINAL.pdf.*

[74] Catherin Stinson. 2018. Healthy Data Policy solutions for big data and AI innovation in health. Mowat Centre. *https://munkschool.utoronto.ca/mowatcentre/wp-content/uploads/publications/179_healthy_data.pdf.*

[75] International Chamber of Commerce. 2015. Cyber Security Guide for Business. *https://cdn.iccwbo.org/content/uploads/sites/3/2015/08/ICC-Cyber-Security-Guide-for-Business.pdf.*

[76] Principles for Digital Development. How to Secure Private Data Stored and Accessed in the Cloud. *https://digitalprinciples.org/wp-content/uploads/PDD_HowTo_SecureCloudData-v2.pdf.*

[77] Accenture. 2019.

CHAPTER III CYBERSECURITY

GOVERNMENT DATA AND CRITICAL INFRASTRUCTURE

Governments have access to large amounts of sensitive information about residents and businesses, and the ongoing digitization of public services is creating more opportunities for cybercriminals to access that data. Most government employees (at least federal and provincial ones) are required to undergo some level of cybersecurity training. Local governments are generally less resourced and therefore more vulnerable. In fact, multiple municipalities in Ontario have fallen victim to ransomware attacks in recent years.[78]

The Government of Ontario follows a set of cybersecurity standards when it procures digital services, which are often higher than those of smaller municipal governments and broader public sector organizations. Using provincial procurement vehicles is one way for other public organizations in Ontario to improve their security postures. This has the added benefit of allowing the provincial government to negotiate lower prices.

POLICY RECOMMENDATION

Municipal governments in Ontario should consider using Government of Ontario procurement vehicles for digital services when provincial cybersecurity standards are higher than their own.

Additionally, governments would benefit from continuously exchanging information about both threats and solutions. The Association of Municipalities of Ontario has begun collecting and sharing information on threats and best practices among its members. Federal and provincial governments should facilitate and participate in such efforts. While not all solutions will be appropriate for all governments, having access to more information will allow each one to make better decisions.

POLICY RECOMMENDATION

Federal, provincial, and municipal governments should exchange information on an ongoing basis about public sector cybersecurity threats and defence techniques.

Critical infrastructure – including energy, telecommunications, transportation, and health – also face a heightened level of risk, as breaches can compromise public safety and national security. The Canadian Centre for Cyber Security is partnering with private and public owners of critical infrastructure to manage these risks.

POLICY RECOMMENDATION

Federal, provincial, and municipal government owners of critical infrastructure should partner with the Canadian Centre for Cyber Security to share threat information and support the integration of cyber defence technology as appropriate and in a manner consistent with privacy obligations.

BEST PRACTICE

Industry owners of critical infrastructure should partner with the Canadian Centre for Cyber Security to share threat information and support the integration of cyber defence technology as appropriate and in a manner consistent with privacy obligations.

[78] David Rider. 2019. "Ontario cities ask feds, province for help repelling ransomware attacks." The Toronto Star. *https://www.thestar.com/news/gta/2019/08/07/ontario-cities-ask-feds-province-for-help-repelling-ransomware-attacks.html.*

CASE STUDY: TD FUSION CENTRE

Financial service providers are faced with rapidly changing cybersecurity environments, geopolitical complexities, and an expanding attack surface as banking becomes increasingly digital. TD Bank Group (TD) responded to these challenges by taking a multi-disciplinary, data-driven approach to protect the data and financial assets of its customers, stakeholders, and the broader economy.

In September 2019, TD launched its Fusion Centre in downtown Toronto, an 8,000 square foot state-of-the-art operational hub that incorporates a best-in-class, multidisciplinary approach to risk management. The hub is focused on improving prediction and prevention of enterprise threats, detecting new threats, and enabling incident response driven by a shared view of TD's threat landscape.

The Fusion Centre relies on cross-functional teams to avoid the siloed nature of threat management that often exists within large organizations. The Centre's "teams of teams" approach integrates different groups from across the Bank, representing cyber operations, incident response, cyber intelligence, information protection services, global security and investigations, fraud management, anti-money-laundering, legal, communications and compliance. Each team brings unique expertise and perspectives to facilitate "shared consciousness" and a culture of collaboration across the organization.

Multi-disciplinary cooperation leads to more effective threat intelligence and faster response times. It allows TD to keep pace with nimble cybercriminals who learn to adjust their tactics and techniques faster than businesses can hire and train employees to respond.

In June 2020, TD will open its Singapore Fusion Centre, while continuing to expand teams and tools across multiple locations. Using a "follow-the-sun model," teams are currently situated in Toronto, New Jersey, Tel Aviv, and Singapore – allowing for continuous coverage across time zones. Ongoing investments in people, processes, and capabilities are informed by best-in-class industry standards such as NIST's Cybersecurity Framework.

TD's approach to threat management is also supported by data, aggregating thousands of disparate data sources through a centralized platform. Artificial intelligence and machine learning tools are coupled with a diversity of employee talents to help improve threat detection and more efficiently protect data and technology assets. TD is also part of a larger network in which cyber threat intelligence and best practices are shared among industry peers, global law enforcement, and government agencies to enhance collective capacity.

Finally, as we all respond to the global implications of COVID-19, TD via the Fusion Centre created a virtual war room to proactively monitor for potential frauds and phishing campaigns related to government relief programs in Canada and the United States. The virtual war room has also been instrumental in helping the bank to coordinate the successful transition of TD's employees from physical locations to working from home as they continue to provide vital banking services to its 25 million customers. By mid-March, TD had approximately 100,000 employees working remotely, up from fewer than 20,000 prior to the pandemic, reflecting the fastest technology pivot in TD's history.

As the threat and cyber landscape grows more complex, TD continues to strengthen its innovative approach to the everchanging environment. The Fusion Centre is an important evolution in TD's ongoing efforts to deliver meaningful innovations that safeguard customers' privacy, security, and trust.

CASE STUDY: CYBERSECURITY & THREAT MANAGEMENT AT SENECA

In January 2020, Seneca launched a new graduate certificate in Cybersecurity & Threat Management. This eight-month program responds to the high demand for skilled cybersecurity professionals in the IT and financial service sectors.

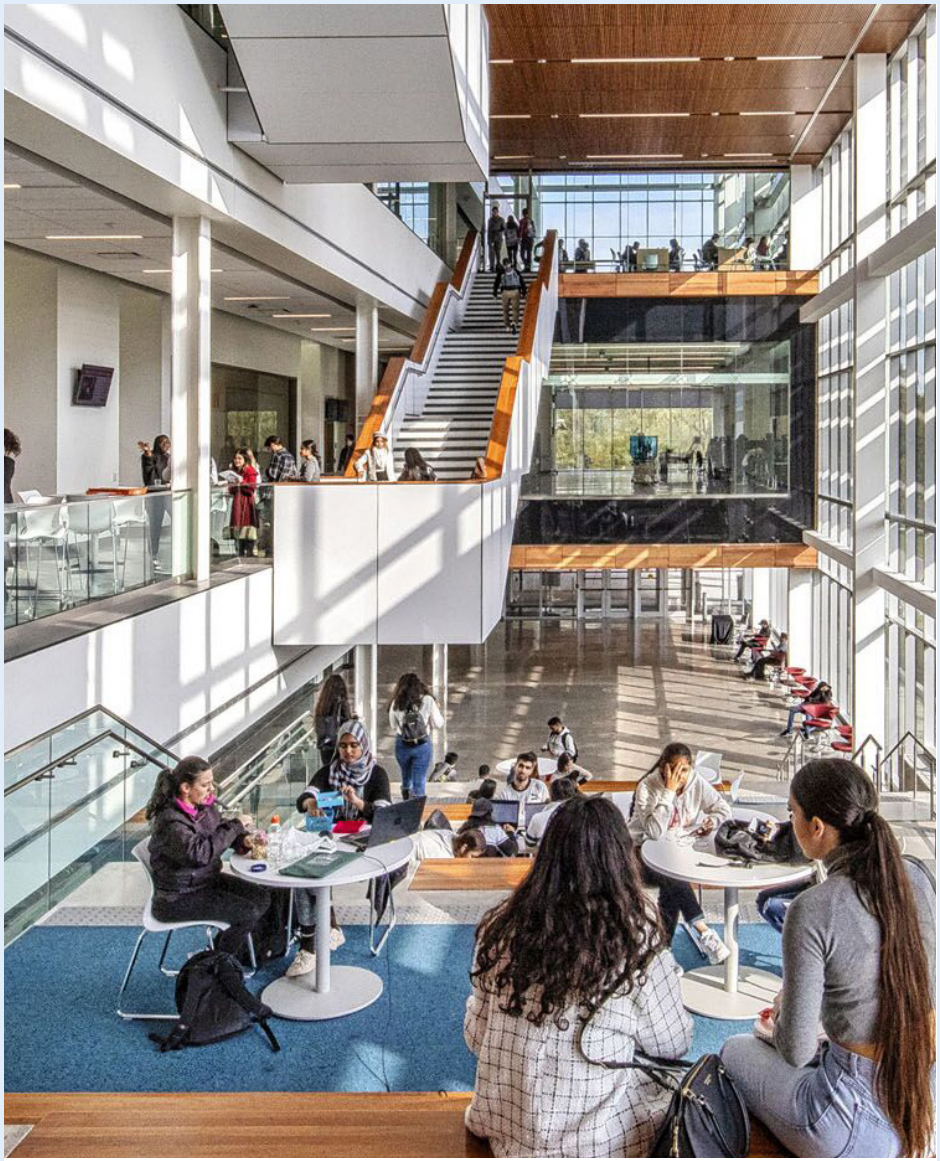
Designed to reflect the industry's cybersecurity needs, the new credential prepares graduates for successful careers in the field. The curriculum was developed in partnership with Toronto Finance International, a public-private partnership between financial institutions, government and academia. Courses are taught by industry professionals, further aligning the skills being taught with the needs of employers.

Most students enrolled in the Cybersecurity & Threat Management program are professionals looking to upskill or reskill. Courses are designed to build technical specialization as well as complementary skills in project management, communication, and data analysis. On site, students are able to practice their knowledge in applied activities in Seneca's new state-of-the-art cybersecurity labs. The program's industry capstone project and optional work term give students additional industry experience that employers often look for.

Graduates are equipped for careers as information security analysts, threat analysts, IT systems and network administrators, risk analysts and ethical hackers. Their skills will directly help address the complex and evolving challenges faced by banks, investment firms, insurance providers and more.

The inaugural intake for the program has been unprecedented with additional spots created to support the demand. Seneca accepts two cohorts per year, starting in January and September. Courses are primarily being offered at Seneca Downtown with the labs delivered at Seneca's Newnham Campus. A part-time option is also available. Courses are delivered in late afternoons, evenings and on Saturdays to accommodate students who are employed.

Through its many industry partnerships, Seneca will continue to adapt the program to reflect the changing cybersecurity needs of employers. This ongoing collaboration with businesses is critical, particularly in a field as rapidly changing, complex and consequential as cybersecurity.



Seneca

CASE STUDY: NERDS ON SITE

Founded in London, Ontario, Nerds On Site is an all-inclusive IT service provider with over 75,000 residential and business clients across North America. What follows is a real example of how Nerds On Site was able to thwart a cybersecurity attack on an international company, bring systems back online with minimal downtime, and secure the company's systems against future attack.

ATTACK

In January 2019, ACME Inc. (not the company's real name) received a ransomware email attachment (a phishing scheme) that launched a PowerShell script – a tool that falls under the radar of traditional endpoint security products. Over the next six months, the undetected threat continued to infect systems across the company's global locations.

ASSESSMENT AND RESPONSE

In July, after realizing they were under attack, ACME Inc. contacted Nerds On Site. The Incident Response Team quickly responded, assessed the situation, and found that ransomware had not yet been deployed. Isolation steps were then taken, prompting attackers to launch the ransomware encryptor, which the Incident Response Team immediately detected. The encryptor and ransom note (demanding $600,000, increasing by $120,000 per day) warned against shutdown and internet disconnection, but the team did just that, shutting down every device in the data centre and the internet connection itself. This allowed full preservation of at least one Active Directory domain controller.

Nerds On Site relied on its Three-Phase Incident Response Protocol:

• Phase One (Isolate): existing Cisco ASA gateways at site-to-site VPN infrastructure were removed and replaced with adam:ONE, a DNS-based firewall and gateway solution.

• Phase Two (Remediate): computers were set up to boot into safe mode, and Webroot was deployed to do a thorough scan. Global IT teams were given step-by-step instructions in their respective languages, communicated across a central dashboard. Once Webroot removed infections, the system was re-scanned to ensure a clean status.

NERDS ON SITE®
TECHNOLOGY PARTNERS

• Phase Three (Fortify and Maintain): adam:ONE technology was used to reconfigure the systems using whitelisting. In contrast to blacklisting, this approach begins from a zero-trust standpoint and only allows users to access resources that have been determined to pose no threat (whitelisted).

RESULTS

Rapidity on the part of the Nerds On Site Incident Response Team stopped the attackers in their tracks. Systems were brought back online with only one shift of downtime and without paying the ransom. Importantly, the team deployed advanced technologies to ensure ACME Inc. is properly fortified against future attacks.

CHAPTER IV

DATA SHARING

Although our digitally connected society makes it easier than ever before to collect colossal amounts of information, most of that data is never processed or used. Instead, valuable data is trapped within silos, where a lack of shared standards, infrastructures, and/or incentives prevent it from being used to its full potential.

This is a major lost opportunity. One study by McKinsey and Company estimated that sharing data more openly across public and private organizations could yield more than $4 trillion per year in additional economic value across seven sectors: education, transportation, consumer goods, electricity, oil and gas, health care, and consumer finance. [79]

Data sharing at a large scale allows for more powerful analyses and new insights. Easier access to data can help accelerate AI training and improve the accuracy of outcomes. With aggregated datasets, firms can identify market segments and customize their services to meet the needs of different groups. Smaller companies and entrepreneurs can overcome information gaps to compete more effectively with larger market players. Consumers might be the ones who benefit the most from data sharing, with increased transparency and lower prices.

At the same time, data sharing can pose a threat to privacy and increase the risk of security breaches. As governments and organizations work towards sharing more information, they must develop appropriate standards and infrastructure to manage those challenges.

[79] McKinsey and Company. 2013. Open Data: Unlocking Innovation and Performance with Liquid Information. *https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Open%20data%20Unlocking%20innovation%20and%20performance%20with%20liquid%20information/MGI_Open_data_FullReport_Oct2013.ashx.*

BUSINESSES AND RESEARCH INSTITUTIONS

As businesses gradually embrace the idea of data sharing, different sectors are developing systems to transfer information efficiently and securely. In Ontario, these initiatives have been voluntary and industry-led, with solutions tailored to how particular sectors use data and the systems they have in place. The extent to which a company chooses to share their data assets can – and should – vary depending on considerations of privacy, security, and IP.

Part of the solution from a technical perspective involves the development of application programming interfaces (APIs), which allow data to be shared securely. The financial services sector is one of several moving towards the development of common API interfaces. Although APIs are the gold standard, they are not necessary for data sharing. Organizations can begin unlocking the benefits by releasing their data in whichever format is convenient, as long as privacy and security obligations are maintained.

Academic institutions are also moving towards more extensive data sharing. This has been driven, in part, by international research communities' efforts to collaborate more effectively, and partly by individual colleges and universities that are taking the lead in releasing their own research data. The University of Guelph, for instance, is developing a platform to make its agricultural data available to industry and other interested third parties.

Another growing trend is data philanthropy, where companies share their private data assets with others for the public good.[80] Businesses often possess a treasure trove of data that can help researchers and policymakers address social issues more efficiently. In return, companies can demonstrate good corporate social responsibility at a relatively low cost and often in a way that aligns their philanthropy with their core commercial activities.[81]

Recent developments are promising, but there is opportunity for more data sharing in Ontario. One solution is to establish large data libraries, where different organizations can pool their data and make it available to researchers to build AI models and glean better insights.[82] At least initially, it might make sense to develop data libraries within specific sectors or around particular types of data, such as natural resources. From a governance perspective, the data trust model discussed in Chapter II could be used to manage access and use, and learnings from the experience can be used to inform approaches used within more sensitive sectors such as health care.[83]

Organizations will need to be conscientious about preserving privacy and security as they share more data. With anonymized data, the risk of re-identification needs to be addressed with best practices. Governments and regulators can help organizations participate by providing guidance around the disclosure of different kinds of information, including de-identified data. While the IPC and the OPC can offer some general advice, industry regulators are ideally placed to provide more specific information and support that is relevant to their sectors.

POLICY RECOMMENDATION

The Governments of Ontario and Canada should work with organizations to clarify privacy and security expectations around data sharing in different sectors.

BEST PRACTICE

Businesses and research institutions should share data where possible while maintaining privacy and security, including through robust de-identification measures, and contribute to collaborative data sharing initiatives such as data libraries and the development of standards.

[80] Brice McKeever, Solomon Greene, Graham MacDonald, Peter Tatian, and Deondre Jones. 2018. Data Philanthropy: Unlocking the Power of Private Data for Public Good. Urban Institute. *https://www.urban.org/sites/default/files/publication/98810/data_philanthropy_unlocking_the_power_of_private_data_for_public_good_0.pdf.*

[81] Ibid.

[82] Canada's Economic Strategy Tables. 2018. The Innovation and Competitiveness Imperative: Seizing Opportunities for Growth. *https://www.ic.gc.ca/eic/site/098.nsf/vwapj/ISEDC_SeizingOpportunites.pdf/$file/ISEDC_SeizingOpportunites.pdf.*

[83] Canadian Institute for Advanced Research (CIFAR). 2020. Report on Canada-US AI Symposium on Economic Innovation. *https://www.cifar.ca/docs/default-source/ai-society/canada-us-ai-symposium-on-economic-innovation/report-on-canada-u-s-ai-symposium-on-economic-innovation.pdf?sfvrsn=86ff0f87_6.*

CHAPTER IV DATA SHARING

HEALTH DATA

Sharing data efficiently is an especially important objective for Ontario's health care sector, where silos are one of the main barriers to improving the quality of care. Information sharing along the continuum of care enables coordination, personalization, and better outcomes for patients. Meanwhile, allowing researchers to access health data can result in new insights, operational efficiencies, and innovation in health care delivery. It also generates new IP, which contributes to the competitiveness of Ontario's health and life sciences sectors.[84]

During a public health crisis, the ability to share data easily only becomes more critical. This recently became evident during the COVID-19 pandemic, where information aggregated across jurisdictions has been used to track, understand, and ultimately contain the spread of the virus. The same is true for the opioid epidemic and other public health crises.

Data sharing within health care is becoming both easier (thanks to digitization) and more valuable (because of advanced data analytics tools). In fact, electronic health records (EHRs) are seen as basic building blocks for health care innovation.[85] EHRs are lifetime records that describe a person's health history and care, with information from a variety of sources, including hospitals, clinics, doctors, pharmacies, and laboratories.[86] By contrast, electronic medical records (EMRs) are individual patient records created by health care providers following specific encounters with patients, and they can serve as a data source for an EHR.[87]

Sharing health data is a tremendous opportunity, but one that needs to be managed carefully because of the sensitive nature of personal health information. Health status should not affect one's access to employment, housing, or other essential services. Many people are also wary of commercial uses of health data and would object to seeing advertisements targeted at them based on that information. Protecting patient privacy in the health care context is also fundamentally about trust; people who do not trust their health care providers may avoid accessing the services they need or choose to access them outside the regulated health care system.

PHIPA outlines certain privacy constraints around sharing health care data in Ontario. Health information custodians, such as doctors and hospitals, may share a patient's personal health information within the patient's circle of care without his or her explicit consent, though they do require consent to share that information directly with researchers or companies.

[84] Sachin Aggarwal. 2018. "Treasure of the Commons: Global Leadership Through Health Data." Centre for International Governance Innovation. *https://www.cigionline.org/articles/treasure-commons-global-leadership-through-health-data.*

[85] Stinson. 2018.

[86] Office of the Auditor General of Canada. 2010.

[87] Habib. 2010.

PHIPA also names a number of prescribed entities – including Cancer Care Ontario (now part of Ontario Health) and the Institute for Clinical and Evaluative Sciences (ICES) – that are authorized to collect health care data from custodians without explicit patient consent for select purposes, such as system administration and public health research. These entities can then share de-identified datasets with researchers and businesses that carry out their own research. ICES, for example, has ongoing projects with Amgen Canada Inc., Janssen Inc., Sunnybrook Research Institute, and others. Prescribed entities are overseen by the IPC, which regularly reviews their privacy practices.

In Ontario, certain types of health data are centralized through eHealth Ontario (now part of Ontario Health), through its Acute and Community Care Clinical Data Repository, Diagnostic Imaging Repositories, Digital Health Drug Repository, and the Ontario Laboratories Information System.

However, information sharing between providers (such as physicians and hospitals) is typically done on an ad hoc basis and impeded by the existence of inconsistent standards and technologies.

When data is shared with third parties (i.e. not health care providers), the process is managed through data sharing agreements (DSAs) and research ethics boards. ICES alone has hundreds of DSAs with different providers. Since DSAs are not standardized documents, each contract must be applied and amended individually in what is often an onerous and expensive process.

Recently, Ontario has taken meaningful steps to facilitate sharing of health data while protecting patients' privacy. Several amendments have been introduced to make it easier for government to access health information through Bill 138, the Plan to Build Ontario Together Act, 2019. These provisions will continue to protect patient privacy by requiring de-identification and mandating that the IPC review each unit's practices.

More recently, in response to the COVID-19 pandemic, the Province amended PHIPA to give individuals more access and control over their health records using digital tools such as apps. The IPC was given oversight over these digital service providers and the power to ensure patient privacy remains protected.[88]

Ontario's transition to a more digital and integrated health care system is imperative. The long-term success of this process will depend on having strong governance frameworks that protect patients while also enabling flexibility and innovation.

To that end, there is a need to clarify and harmonize standards around sharing of health data. Part of the challenge is finding consensus around privacy obligations. For example, as in other sectors, there is a question of how much consent is necessary when sharing personal data that has been anonymized or de-identified. One option is to require explicit consent from patients whenever their data is shared for secondary purposes not directly related to health. Alternatively, it may be deemed sufficient to obtain broad consent to use a patient's information for a variety of unspecified research purposes – a practice that is becoming more common.

De-identified data has typically not been considered personal health information from a privacy perspective, but a growing body of evidence suggests anonymized data can be re-identified in many cases. Data custodians should have clear information about any additional privacy protections they should adopt to help prevent re-identification. There are also unique considerations around sharing biometric data, which is identifiable by nature.

Further, are there scenarios in which sharing *identifiable* information should be allowed without explicit consent? For example, health insurance companies require identifiable data in order to audit claims to prevent fraud. However, health care providers are not confident that PHIPA allows them to rely on general consent from health plan members to investigate suspicious claims. Clarification in this case is essential to ensure insurance companies are able to effectively prevent, detect, and suppress fraud.

[88] Brian Beamish. 2020. "How government's response to COVID-19 ushered in new privacy protections." IPC. *https://www.ipc.on.ca/how-governments-response-to-covid-19-brought-in-new-privacy-protections/.*

There is also a need to establish very clear rules around commercial uses of health data. In the United Kingdom, for example, data can only be shared with businesses when it has the explicit aim of improving the health, welfare, or care of patients or improving the operation of the national health care system. When data is shared with companies, there should be clear, standardized processes and protections in place.

Agreeing on clear and consistent standards is only part of the solution. Facilitating data sharing within Ontario's health care system also requires shifting towards a more integrated data management system in which interoperable standards and technologies are used consistently across the health care system. This is an infrastructure challenge.

The main gaps in data sharing are seen with EMRs. Currently, for example, general practitioners and hospitals are not efficiently and automatically sharing information about patients. Different health care providers use different digital systems that code information in incompatible ways.[89] Patients can access their information online, but mostly through siloed portals set up by individual institutions.[90] While robust standards do exist, they are not leveraged effectively across the system.

Ontario's efforts to integrate health data are promising. However, centralization is an ambitious objective that will take time and should be prioritized as Ontario transitions to a more integrated health care system.[91] It will require convergence around technical standards, IT systems, and consent management policies. Interoperability will need to be rolled out across more infrastructure, including identity verification for patients accessing digital health services. It may also require incentives for EMR vendors.

Privacy by design should be a core feature of the system. Patient should be able to easily issue consent directives to control who can access their personal health information. One of the benefits of interoperable technology is that it enables patients' consent preferences to be applied more quickly and easily across the system. As an example, the United Kingdom's National Health Service has recently introduced a national data opt-out, which applies patients' consent preferences across all health and social care organisations. De-identification should also be built into the system to ensure personal information is automatically protected with best-in-class anonymization techniques.

Decisions around how health data is shared will have material impacts on patients, providers, and the health care system at large. Therefore, it is important that this transition be characterized by transparency and collaboration. One option is for the Government of Ontario to establish a multi-stakeholder stewardship body responsible for overseeing the sharing of health data in Ontario. This idea was proposed by the Ontario Medical Association based on a similar model used in Alberta.[92]

[89] EStinson. 2018.

[90] Dan Sheldon. 2016. "Digital health in Ontario: An international comparison." Public Digital. *https://files.ontario.ca/26._dan_sheldon.pdf.*

[91] Ontario Ministry of Health. 2020. "Ontario Health agency." *https://www.ontario.ca/page/ontario-health-agency.*

[92] Ontario Medical Association. 2019. "Amendments to O.Reg 329/04 (General) under PHIPA." (Submission to Ontario's Ministry of Health).

The committee's responsibilities could include promoting convergence around standards and making policy recommendations. Unlike the IPC, which oversees the legislation, this group would focus specifically on data sharing mechanisms, including DSAs and EHRs, where there is currently a lack of coordination and oversight. Standardization may occur through a combination of regulations, codes of practice, and/or guidance. As the Ontario Health Teams roll out their digital health integration, clear guidance will ensure consistent adoption of standards and solutions across the province.[93]

Currently, Ontario's eHealth Standards Program offers guidance on selecting the right interoperability standards when implementing EHR solutions.[94] Health care providers should take advantage of such tools while broader efforts are made to update the system.

Representation on the committee should consist of a variety of stakeholders, including health care delivery organizations, life science companies, health technology firms, policymakers, and members of the public. Public representation would help to improve transparency, trust, and public awareness around data sharing. The body should be arm's length from government, providing it with the autonomy needed to make impartial recommendations. The committee should also work alongside, and in collaboration with, other standard-setting organizations, including the Health Standards Organization and the Standards Council of Canada, to continuously refine standards and expectations.[95]

POLICY RECOMMENDATION

The Government of Ontario should continue transitioning towards a more centralized data management system for health care information by working with stakeholders to harmonize standards and technologies required to effectively share health data. This process could be informed by an arm's length stewardship committee.

BEST PRACTICE

Health stakeholders should support adoption of consistent standards around the sharing of health data.

In the long-term, Ontario should look beyond provincial borders with a view to supporting a national system to link and share health data. As demonstrated by the COVID-19 pandemic, it is naïve to try to manage public health within regions in isolation. The scope of health information exchanges should extend nationally, if not internationally.[96]

The current fragmentation between provinces is a challenge in many respects. The Advisory Council on the Implementation of National Pharmacare has noted, for example, that fragmented and incomplete data on prescription drugs makes it difficult to understand how Canadians use drugs and identify inefficiencies and gaps in care.[97] With better data linkages, Canada's network of publicly funded health care systems could offer researchers an abundance of valuable population-level information. The possible expansion of public drug coverage schemes and the digitization of health are opportunities to unlock that potential. As each province works to develop their own digital health standards, it is now more important than ever to coordinate across Canada.

There are initiatives underway to develop interprovincial standards and systems, including work being undertaken by the Canadian Personalized Health Innovation Network (CPHIN). Provincial governments, with the support of the federal government, should support and build on that work.

POLICY RECOMMENDATION

The Governments of Canada, Ontario, and other provinces should collaborate to accelerate systemic, nationwide sharing of health data.

[93] Government of Ontario. 2019b. Ontario Health Teams: Digital Health Playbook. *http://health.gov.on.ca/en/pro/programs/connectedcare/oht/docs/dig_health_playbook_en.pdf.*

[94] eHealth Ontario. 2013. Standards Selection Guide. *https://www.ehealthontario.on.ca/images/uploads/pages/documents/eHealth_Standards_Selection_Framework_en.pdf.*

[95] Aggarwal. 2018.

[96] Niam Yaraghi. 2020. "The US lacks health information technologies to stop COVID-19 epidemic." The Brookings Institute. *https://www.brookings.edu/blog/techtank/2020/03/13/the-u-s-lacks-health-information-technologies-to-stop-covid-19-epidemic/.*

[97] Health Canada. 2019. A Prescription for Canada: Achieving Pharmacare for All. *https://www.canada.ca/en/health-canada/corporate/about-health-canada/public-engagement/external-advisory-bodies/implementation-national-pharmacare/final-report.html.*

GOVERNMENTS: OPEN DATA

Open data is an important principle for modern democracies, where sharing government data with individuals has immense potential to improve transparency and spur innovation.

Through its Open Data Directive, the Government of Ontario has committed to taking an open-by-default approach by requiring government data to be public unless exempted for specific reasons. The Government of Canada has an extensive open data system, and municipalities within Ontario have also embraced it to varying degrees.

Further, *Ontario's Simpler, Faster, Better Services Act, 2019* is focused on improving digital and data services in Ontario, in part by establishing and promoting open data standards for government and the broader public sector. One of the ways the Ontario Digital Service is enabling data sharing is by adopting APIs at the outset when developing digital services.[98]

Ontario's open data catalogue a step in the right direction, but there is room for improvement. First, the data should be released more immediately, when it is most valuable to citizens and businesses. Indeed, data scientists would much prefer to see government data released early and messy than later in a standardized format, allowing them to cleanse the data according to their unique needs.

Second, there is a need for a broader range of data to be released. Provincially, this should extend to open contracting, whereby government publishes complete information about the planning, decision making, scoring, and awarding of all government contracts. There is evidence that open contracting leads to more innovation and better value-for-money, as well as higher levels of public trust.[99]

Another opportunity to improve transparency is with proactive disclosure of certain completed freedom of information requests (subject to strong privacy and ethical conditions), which would also significantly reduce the administrative costs associated with meeting those requests. The City of Toronto and the Government of Canada already publish summaries of completed requests.[100]

[98] Paul Vet. 2019. "Ontario's new API Guidelines: How to create the building blocks of government on the internet." Ontario Digital. https://medium.com/ontariodigital/ontarios-new-api-guidelines-how-to-create-the-building-blocks-of-government-on-the-internet-d772c6101ced.

[99] Open Contracting Partnership. "Evidence: How open contracting improves key government services." Accessed March 2020. https://www.open-contracting.org/impact/evidence/.

[100] IPC. 2019. "Re: Government of Ontario's Creating Economic Benefits Discussion Paper" (Letter to Minister Thompson). https://www.ipc.on.ca/wp-content/uploads/2019/10/2019-10-15-ltr-to-minister-lisa-thompson_mgcs_re-creating-economic-benefits-paper.pdf.

CHAPTER IV DATA SHARING

The need to expand the breadth of open data is particularly salient at the municipal level. ThinkData Works has compiled a list of core datasets that most municipalities in Ontario have access to, but few openly share.[101] This includes information about:

- Infrastructure (land parcels, construction activity, parking lots, air travel, etc.)
- Economy (business activity, economic indicators, utility usage, housing development, etc.)
- Environment (pollution, floodplains, orthophotography, etc.)
- Civic services and public safety (health care facilities, city services, public housing, etc.)
- Government (demographics, census information, licensing, government buildings, etc.)
- Society and culture (cell towers, events, cultural facilities, etc.)

The City of Toronto's open data catalogue is seen as exemplary. It includes a wide range of datasets as well as open-source software that other local governments can use to reduce the costs of publishing their data. The open data websites of both the City of Toronto and the Government of Canada also offer many practical examples of how their data has been used, giving inspiration to new uses and users. The Ontario government can also help municipalities improve their open data systems with technical support, guidance around privacy and security, and information on the benefits for their communities.

Finally, the best way to ensure open data systems are useful and accessible is to have ongoing dialogue with external users through a feedback loop that can involve both formal and informal channels of communication. Alberta's open data system has been appropriately praised in this regard. The COVID-19 crisis, throughout which the Ontario government has worked with external researchers to respond to urgent data access needs, could serve as a catalyst for long-term collaboration.

POLICY RECOMMENDATIONS

The Government of Ontario should improve upon both the speed and breadth of its open data. Practices should include open contracting and proactive disclosures of completed freedom of information requests.

Ontario's municipal governments should release a broader range of datasets. The Government of Ontario should encourage and facilitate these efforts with technical support, guidance around privacy and security, and information on the benefits for communities.

The Government of Ontario should establish a feedback loop with open data users to facilitate ongoing improvements to its catalogue.

[101] Lewis Wynne-Jones. 2019. "The Data Every City Should Release and Why." ThinkData Works. *https://blog.thinkdataworks.com/data-every-city-should-release.*

CHAPTER V

ARTIFICIAL INTELLIGENCE

One of data's most valuable qualities is its ability to power artificial intelligence (AI) and AI's more advanced subset, machine learning (ML). AI is a general-purpose technology that underpins autonomous vehicles, modern financial services, smart cities, and a plethora of other use cases across the economy. In the long-term, widespread adoption of AI and ML is expected to raise productivity and output, create more jobs than it replaces, and lower prices for consumers.[102]

"One thing is certain: whether directly or indirectly, AI systems play a key role across businesses and shape the global economy for the foreseeable future."

– Artificial Intelligence Index Report 2019 [103]

[102] Stephen S. Poloz. 2019. Technological Progress and Monetary Policy: Managing the Fourth Industrial Revolution. Bank of Canada. *https://www.bankofcanada.ca/wp-content/uploads/2019/11/sdp2019-11.pdf.*

[103] Raymond Perrault, Yoav Shoham, Erik Brynjolfsson, et al. 2019. The AI Index 2019 Annual Report. Stanford University. *https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf.*

CHAPTER V ARTIFICIAL INTELLIGENCE

For over thirty years, Canada has been recognized as a global leader in AI. In 2017, Canada became the first country in the world to adopt a national AI strategy.[104] The Pan-Canadian AI Strategy, developed by the Canadian Institute for Advanced Research, aims to expand the number of AI researchers and skilled graduates, establish interconnected notes of scientific excellence, develop thought leadership on the socioeconomic implications of AI, and support a national AI research community.[105]

Ontario, in particular, is home to some of the world's most advanced AI research networks and a thriving ecosystem for AI startups. Geoffrey Hinton, known as the grandfather of ML, is one of several experts based in Toronto, where he is a Chief Scientific Advisor at the Vector Institute. Many of Ontario's firms have successfully scaled and expanded internationally, such as MindBridge – an Ottawa-based company responsible for creating the world's first AI-powered auditing solution.[106] Ontario's advantage will only become more important in the increasingly intangibles-based economy, where ownership of AI firms, talent, and IP will drive competitiveness.

Autonomous vehicles are one field of AI in which Ontario took early steps to position itself as a leader, investing heavily in the technology and becoming the first jurisdiction in Canada to introduce a pilot regulatory framework.[107] With driverless technology poised to revolutionize personal mobility, transportation networks, and auto manufacturing, maintaining a competitive advantage in this space is both an economic and societal opportunity.

However, the province faces three main challenges when it comes to AI. First, as discussed in Chapter IV, easier data sharing is necessary to give innovators access to the large datasets required to develop AI models. Second, Ontario must go beyond its existing advantages in AI research to accelerate commercialization and technology adoption. Third, policymakers need to commit to a governance approach that supports innovative yet responsible application of the technology.

AI APPLICATIONS IN HEALTH CARE AND THE COVID-19 EXAMPLE

Among AI's array of applications, there are many benefits for health care. The technology's value largely stems from its ability to combine data from multiple data sources to arrive at quicker and better insights than even the best medical professionals could. This includes data from electronic records, clinical trial reports, administrative files, insurance, personal health devices, public health statistics, and more.

AI's impact on medical imaging has already been significant, allowing for quicker and cheaper diagnostics, sometimes bypassing the need for a highly skilled specialist. AI can also allow for more personalized treatment plans, faster clinical trials, and supply chain optimization.

The COVID-19 pandemic has brought new urgency and attention to this conversation, beginning early on when news articles reported that AI was able to detect the outbreak before public health officials.[108] It is important not to exaggerate the role AI can play in a pandemic; since good algorithms require a lot of prior data and models need to be externally validated, it works better for detailed tasks than big-picture ones.[109] That said, AI could realistically be deployed to allocate health care resources more efficiently by predicting which patients will require ventilation, accelerate the drug discovery process, target information to segmented audiences, and identify fake news.[110]

Finally, while the pandemic has illustrated the benefits AI can have on health care, it has also underscored the difficulty AI researchers have accessing health data.[111] The Ontario government's development of the Ontario Health Data Platform (discussed in Chapter I) is one attempt to facilitate that access.

[108] Will Douglas Heaven. 2020. "AI could help with the next pandemic–but not with this one." MIT Technology Review. *https://www.technologyreview.com/s/615351/ai-could-help-with-the-next-pandemicbut-not-with-this-one/.*

[109] Alex Engler. 2020. "A guide to healthy skepticism of artificial intelligence and coronavirus." The Brookings Institute. *https://www.brookings.edu/research/a-guide-to-healthy-skepticism-of-artificial-intelligence-and-coronavirus/.*

[110] Kate Allen. 2020. "AI scientists are mobilizing to combat coronavirus. Here's how the provinces are holding them back." The Toronto Star. *https://www.thestar.com/news/gta/2020/03/24/ai-scientists-are-mobilizing-to-combat-coronavirus-heres-how-the-provinces-are-holding-them-back.html;* and Cheryl To. 2020. "Using Data to Combat COVID-19." ThinkData Works. *https://blog.thinkdataworks.com/using-data-to-combat-covid-19.*

[111] Allen. 2020.

CHAPTER V ARTIFICIAL INTELLIGENCE

AI IN NUMBERS

$90 BILLION
GLOBAL INVESTMENT IN AI IN 2019.[112]

$200 BILLION
CHINESE GOVERNMENT'S INTENDED INVESTMENT IN AI (2018-2030).[113]

$2.9 TRILLION
GLOBAL BUSINESS VALUE CREATED FROM AI IN 2021.[114]

OVER 300
AI START-UPS LOCATED WITHIN THE TORONTO-WATERLOO REGION.[115]

190%
INCREASE IN NUMBER OF JOBS REQUIRING AI SKILLS BETWEEN 2015 AND 2017.[116]

83%
OF CANADIAN C-SUITE EXECUTIVES BELIEVE THEIR COMPANIES MUST LEVERAGE AI TO ACHIEVE THEIR GROWTH OBJECTIVES, YET...

89%
SAY THEY STRUGGLE WHEN IT COMES TO SCALING AI ACROSS THE BUSINESS. [117]

COMMERCIALIZATION AND TECHNOLOGY ADOPTION

While Ontario excels at innovative AI research, it underperforms when it comes to commercialization and industry adoption of the technology. The province needs to do better, or it risks providing other countries with research that fuels their growth without realizing the benefits locally.[118]

In terms of commercialization, Canada produces fewer patents and other forms of IP than its international peers, and a significant portion of its IP ends up in foreign ownership.[119] In early 2020, Ontario's Expert Panel on Intellectual Property made a series of recommendations to help mitigate the commercialization gap.[120]

Limited AI adoption within the economy is another missed opportunity. Beyond its direct benefits for businesses, technology adoption raises overall economic productivity, wages, and living standards. A 2019 survey by Deloitte Canada revealed that only 16 percent of Canadian businesses have adopted some form of AI, a number that remains unchanged since 2014.[121]

[112] Perrault et al. 2019.

[113] Darrell M. West and John R. Allen. 2018. "How artificial intelligence is transforming the world." The Brookings Institute. https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/.

[114] Gartner. 2019. "Gartner Says AI Augmentation Will Create $2.9 Trillion of Business Value in 2021." https://www.gartner.com/en/newsroom/press-releases/2019-08-05-gartner-says-ai-augmentation-will-create-2point9-trillion-of-business-value-in-2021.

[115] Jason Kirby. 2018. "Canada's Next Breakthrough is AI Commercialization." MaRS Discovery District, https://www.marsdd.com/magazine/canadas-next-breakthrough-is-ai-commercialization/.

[116] Igor Perisic. 2018. "How artificial intelligence is shaking up the job market." World Economic Forum. https://www.weforum.org/agenda/2018/09/artificial-intelligence-shaking-up-job-market/.

[117] Accenture. 2019. AI: Built to Scale. https://www.accenture.com/us-en/insights/artificial-intelligence/ai-investments.

[118] Claudia Krywiak. 2020. "Canadian AI Tech: From R&D to Commercialization." The Future Economy. https://thefutureeconomy.ca/spotlights/sp-ai-for-smes/claudia-krywiak/.

[119] Asselin and Speer. 2019.

[120] Jim Balsillie, Shiri M. Breznitz, Myra Tawfik, Dan Herman, and Natalie Raffoul. 2020. Intellectual Property in Ontario's Innovation Ecosystem (Report to the Government of Ontario). Expert Panel on Intellectual Property. https://files.ontario.ca/books/expert-panel-report-intellectual-property-2020-02-20_0.pdf.

This reluctance to adopt AI can be explained by regulatory uncertainty, a culture of risk aversion, difficulty accessing late-stage capital, access to skills, limited understanding of AI's benefits, and low levels of overall business investment in technology.[122] To support greater technology adoption, federal and provincial governments have offered funding through Innovative Solutions Canada, the Strategic Innovation Fund, and Ontario Centres of Excellence, among others.

It is important that governments continue to fund primary AI research as well as applied research that engages end users and facilitates practical implementation of the technology. Partnerships between industry and academia can help to ensure that AI applications are both relevant to industry needs and more easily adopted within Ontario.

Federal and provincial governments can also direct more of their innovation programs towards scale-up firms: small, innovative firms that are growing at a rate of at least 20 percent per year.[123] These businesses have demonstrated a high potential for growth and face very specific challenges, including expanding into diverse global markets and accessing long-term capital.[124]

Both governments should also work on harmonizing the supports they offer. A whole-of-government approach would ensure companies applying for one program are automatically considered for relevant supports by other departments and agencies.

Another way for governments to support AI is by leveraging their procurement processes. As the largest customer in the economy, government can use AI to modernize internally while helping technology firms scale more efficiently than with tax credits or grants. The US government has invested heavily in procuring AI, with federal agencies spending a combined $975 million on AI-related contracts in 2018, an increase of nearly 70 percent from the year before.[125]

There are several ways public-sector buyers in Ontario can take a more innovation-oriented approach to procurement. These include using proofs of concept to test the technologies before the final purchase or adopting challenge-based procurement systems.[126] Using procurement to support AI development is not only an opportunity for governments, but also for large corporations to integrate more innovative SMEs within their supply chains.[127]

Ontario businesses can also help accelerate adoption by embracing open-source AI, though this may not be appropriate in all cases. At a minimum, businesses that are familiar with using AI should share information about their experiences to help other organizations understand the technology better and improve leadership buy-in.[128] Non-adopters should evaluate the applicability of AI to their businesses, especially those in industries with traditionally low rates of adoption, such as law and construction.[129]

[121] Deloitte Canada. 2019. Canada's AI imperative: From predictions to prosperity. *https://www.canada175.ca/sites/default/files/download/files/18-5963M_FCC_Omnia_Report_POV_Print_VF_JPC_AODA_863713.pdf.*

[122] Ibid.

[123] David A. Wolfe. 2019. A Digital Strategy for Canada: The Current Challenge. Institute for Research on Public Policy. *https://irpp.org/wp-content/uploads/2019/01/A-Digital-Strategy-for-Canada.pdf.*

[124] Ibid.

[125] Perrault et al. 2019.

[126] World Economic Forum. 2019. Guidelines for AI Procurement. *http://www3.weforum.org/docs/WEF_Guidelines_for_AI_Procurement.pdf.*

[127] Angela Mondou. 2020. "Canada Must Rethink Education and Regulations to Prepare for the 4th Industrial Revolution." The Future Economy. *https://thefutureeconomy.ca/interviews/angela-mondou/.*

Finally, regional internet access is critical to making sure that AI adoption is possible across the province. Governments and the telecommunications industry each have an important role to play in expanding and upgrading broadband networks, particularly as fifth-generation (5G) capabilities are rolled out around the world.

POLICY RECOMMENDATIONS

The Government of Ontario should support commercialization and adoption of AI within the province by:

- Implementing the recommendations of the Expert Panel on Intellectual Property; and
- Leveraging more innovation-oriented procurement processes internally and across the broader public sector.

The Governments of Ontario and Canada should support commercialization and adoption of AI by:

- Continuing to fund AI research, industry-academia partnerships, and implementation supports for businesses;
- Targeting more support towards scale-up firms;
- Harmonizing the innovation support programs they offer; and
- Embracing a whole-of-government to streamline business supports.

The Governments of Ontario and Canada should continue to work closely with industry to invest in regional internet network expansions and upgrades.

BEST PRACTICE

Businesses that have not adopted AI should evaluate the applicability of AI to their own operations and experiment with its use.

[128] Deloitte Canada. 2019.
[129] Ibid.

CHAPTER V ARTIFICIAL INTELLIGENCE

For most organizations, one of the top barriers to adopting AI is access to the right skillsets. Canada currently ranks 14th out of sixty countries on data skills and 24th on technology skills, though the country outperforms its peers when it comes to ML and human computer interaction.[130] AI talent is a competitive advantage for Ontario in particular, with the University of Toronto ranking highest among non-US schools in its number of registered students enrolled in courses on AI and ML.[131]

Maintaining that advantage will be difficult as demand for that talent grows and employers are forced to compete globally for those limited skillsets. According to a 2018 study, one in four graduates of science, technology, engineering, and mathematics programs from Canada's top universities leave the country for jobs abroad.[132]

Another challenge is helping current workers transition to the new labour market. Automation will not lead to mass unemployment, but it will require upskilling so that people to learn to work productively alongside machines. Policymakers, judges, and other professions will also need a deeper understanding of AI to effectively govern its use.

Currently, businesses looking to recruit AI talent can access supports such as NextED, Vector Institute Scholarships in AI, and the Canada's Global Skills Strategy. Post-secondary institutions also offer degree and certification programs to support development of these skills. Scholarships funded partially by government are a good way to attract talented students to careers in AI.

Collaboration among government, educational institutions, and employers will be essential to build an AI-ready workforce. Since lifelong learning will only become more important in the future, stakeholders should work together to offer more workforce development programs, including nimble virtual and micro-certifications, across sectors and regions. SMEs should be engaged regularly in these initiatives.

Finally, when it comes to AI, diversity and inclusion are imperative. The ethical challenges of AI (discussed below) are best mitigated when a variety of perspectives are involved in its design and use. Canada already has relatively high female representation in AI compared to other countries.[133] Any effort to build on the workforce's data and digital skills should aim for proportional representation from Indigenous peoples, visible minorities, women, and people with disabilities.

POLICY RECOMMENDATIONS

The Government of Ontario should partner with employers and training institutions across the province to support data and digital skills development.

The Government of Ontario should work with stakeholders to ensure diversity and inclusion are factored into workforce development initiatives.

BEST PRACTICE

Organizations should take an active approach to upskilling workers with data and digital skills. A holistic approach should be taken to ensure employees across departments are equipped to work with or alongside AI.

[130] Coursera. 2019. Global Skills Index. *https://www.coursera.org/gsi.*

[131] Perrault et al. 2019.

[132] Asselin and Speer. 2019.

[133] Perrault et al. 2019.

CHAPTER V ARTIFICIAL INTELLIGENCE

GOVERNING AI

While AI can have widespread social and economic benefits, it does raise certain ethical challenges. For instance, there have been numerous cases of AI systems leading to discriminatory outcomes because the data on which they were trained contained implicit biases.[134]

AI also complicates data privacy, and especially the practice of consent, as it often involves using data in ways not originally intended at the time of collection. The risk of re-identification may also be higher when there is a combination of de-identified datasets. However, it is worth noting that AI can help with data security by identifying unauthorized access in real time.

There is also a general sense of unease around the idea that algorithms are making decisions on behalf of humans. Some of this unease will likely go away over time as people become more familiar with AI's applications, but this can only occur if there are structures in place to minimize the real risks. In other words, regulating AI effectively is critical to building long-term trust around the technology.

The EU has reacted by taking a more prescriptive approach. The GDPR includes a 'human-in-the-loop' provision that requires automated decisions to be reviewed by humans when they significantly affect individuals' lives, such as when they decide whether to offer a loan or evaluate an employee's performance. The GDPR also requires organizations to explain how AI systems make decisions (known as the explainability rule).

Many observers argue the GDPR's approach will impede AI innovation in the EU, and many businesses are concerned about the impacts a similar regime would have in Canada. The human review requirement is expensive, especially when applied to more sophisticated AI systems, and could disadvantage smaller firms. It also reduces the business case for adopting AI in the first place.

Further, there is a trade-off between the accuracy of AI systems and their explainability.[135] Critics argue it makes little sense to hold back the adoption of AI systems that make more accurate decisions than humans, simply because you cannot explain them. In the words of Geoffrey Hinton: "Suppose you have cancer and you have to choose between a black box AI surgeon that cannot explain how it works but has a 90 percent cure rate and a human surgeon with an 80 percent cure rate. Do you want the AI surgeon to be illegal?" [136]

[134] Kearns and Roth. 2020.

[135] Alex John London. "Artificial Intelligence and Black‐Box Medical Decisions: Accuracy versus Explainability." The Hastings Centre 49(1): 15-21. https://doi.org/10.1002/hast.973.

[136] @geoffreyhinton. February 20, 2020. Twitter. https://twitter.com/geoffreyhinton/status/1230592238490615816.

CHAPTER V ARTIFICIAL INTELLIGENCE

Governing AI effectively is easier said than done. There is broad consensus that relying entirely on self-regulation is not an approach that breeds public trust. Clear legal safeguards are necessary, both to protect the public and to give industry the regulatory certainty needed to continue investing in the technology.

It is important to have a good understanding of what the real risks are and how existing frameworks address or fail to address them. For example, privacy laws contain provisions around consent, but these need to be clarified within the context of AI (as discussed in Chapter II).

Labour and human rights laws are likely best suited to deal with issues of ethics and discrimination, though they might need to be updated to ensure there is recourse for unwanted outcomes that arise from automated decisions. For example, if AI is being used to make hiring decisions that end up discriminating against some group, there should be a clear path to seek remedy within anti-discrimination laws. Consumer protection laws may need similar revisions.

The question of liability, in particular, needs clarification. To disincentivize potentially harmful applications of AI, it is important that legal obligations do not disappear when machines are replacing humans. For now, it is not entirely obvious from whether legal responsibility for adverse outcomes lies with developers or those deploying the technology. Companies that use third-party AI tools should bear some responsibility for ensuring the tools they procure are ethical; however, they could also have contractual or legal means to share liability with developers when the algorithms are opaque due to proprietary software, patents, and/or general complexity. [137]

A gap analysis will help identify where each issue is best resolved. Federal solutions are almost always preferable to provincial ones to avoid layering or duplication of regulation. Any concerns that are specific to a certain industry, such as health care or financial services, should be addressed within the framework of that sector's existing regulations. [138]

Any attempt to regulate AI should be outcomes-oriented and technology-neutral. It makes more sense to hold organizations accountable for undesirable consequences, with clear and stringent penalties, than to regulate specific technologies in a way that discourages innovation.

Since the risks surrounding AI will likely continue to evolve over time, the review of legal and regulatory frameworks should be an ongoing process informed by businesses, developers, consumer advocacy groups, and other stakeholders with a range of perspectives that may not be fully represented within government.

POLICY RECOMMENDATIONS

The Governments of Ontario and Canada should carry out gap analyses to identify risks around AI and whether they are adequately addressed in current legal and regulatory frameworks. This review should take place on a recurring basis with support from stakeholder advisory committees.

Based on the findings of a gap analysis, the Governments of Ontario and Canada should consider updating legislation and regulation to clarify protections against AI-related risks. Providing clarity around liability should be a priority.

[137] Caitlin Chin. 2019. "Assessing employer intent when AI hiring tools are biased." The Brookings Institute. *https://www.brookings.edu/research/assessing-employer-intent-when-ai-hiring-tools-are-biased/.*

[138] Google. 2019. Perspectives on Issues in AI Governance. *https://www.blog.google/outreach-initiatives/public-policy/engaging-policy-stakeholders-issues-ai-governance/.*

Government policy is not the only solution to AI governance. There are several best practices that organizations should adopt proactively to manage risks when developing or deploying AI, including employee training, transparency, risk assessments, and audits. Organizations should anticipate unintended consequences before they manifest and build redundancy into AI systems to minimize their occurrence. Codes of practice should help to reinforce best practices.

Specific opportunities exist to develop standards around transparency. For example, while there are costs associated with requiring complete explainability, organizations could reasonably commit to disclosing more general, non-commercial information about the inputs they feed into their models, how they account for potential ethical risks, and what steps they take to protect that data. This allows outsiders to identify potential causes for concern, while still protecting IP.

Similarly, standards could encourage human oversight of AI decisions in a way that is broadly proportional to the impact decisions will have on individuals' lives.[139] Codes of practice and certifications may also be helpful to improve training for people tasked with developing and/or using AI models. Organizations should always encourage staff to identify and report potential harms with clear processes in place to respond to concerns while protecting employees.

Various AI standards already exist, such as the CIO Standards Council of Canada's *Ethical Design and Use of Automated Systems*, published in 2019. As with privacy, there are cases in which AI codes and standards can be applied generally and cases in which they should be sector-specific. For example, the Office of the Superintendent of Financial Institutions is updating its regulatory expectations around managing model risk to account for financial institutions' use of the technology.

However, a proliferation of standards across sectors and jurisdictions will only add more confusion. A coordinated approach is needed with emphasis on international collaboration wherever possible. One key initiative is the ISO's work on AI Standards (ISO/IEC JTC 1/SC 42).[140] The OECD has also made progress on this front. The OECD Principles on AI – adopted in May 2019 as the first intergovernmental standard on AI – have influenced public policy in several countries, and the OECD's AI Policy Observatory was recently launched to help policymakers implement these principles and monitor the responsible development of AI around the world. The Government of Canada should continue to engage in this work and ensure that Canadian perspectives and expertise are represented on the international stage.

Finally, as governments procure more AI solutions internally, they too should follow international standards and best practices. The Government of Canada is leading by example with its Directive on Automated Decision-Making and Algorithmic Impact Assessment, a tool to assess and mitigate potential risks associated with the automated systems it adopts internally.[141] Governments at all tiers should work together to share information and resources to procure and use AI responsibly.

POLICY RECOMMENDATIONS

The Governments of Ontario and Canada should help ensure Canadian stakeholders are well represented and given a voice in international standard-setting forums.

The Governments of Ontario and Canada should follow international best practices when procuring AI internally.

BEST PRACTICE

Organizations developing and using AI should work with international partners to advance and adopt responsible AI standards and best practices around risk assessments, transparency, and employee training.

[139] Deloitte Canada. 2019.

[140] ISO. "ISO/IEC JTC 1/SC 42 - Artificial Intelligence." https://www.iso.org/committee/6794475.html.

[141] Government of Canada. 2019c. "Directive on Automated Decision-Making." https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

CONCLUSION: A CALL TO ACTION

Mobilizing data in responsible and innovative ways generates benefits across society. Canada – and Ontario specifically – stand to gain tremendously from the potential of data, but unlocking its value requires trust and protection against the risks it carries.

With public opinion being a major driver of public policy, it is essential for Ontarians to have an evidence-based understanding of data-driven innovation. The reality is that most contemporary goods and services Ontarians rely on are made possible to some extent by data analytics and related technologies, from fraud detection to supply chain optimization. Many consumers may not fully understand the opportunity costs of restricting the use of data, but they would certainly feel its effects.

For this reason, it is important to avoid sensationalized narratives and focus instead on confronting the real threats where they exist. Building data and digital literacy is certainly not a simple task. Clear terms and conditions are helpful, but they might not always have a significant impact on public comprehension or trust. Rather, data should be discussed openly whenever information is exchanged, including in everyday interactions with businesses, health care providers, and government. Individuals will continue to demand strong privacy protections, as they should, but those demands will be driven by facts and values.

Policymakers should support responsible data innovation by applying overarching principles consistent with international best practices. Industry-specific guidelines can improve clarity, where appropriate, without duplicative and overly cumbersome restrictions. Ultimately, organizations and entrepreneurs should have confidence in their ability to use data for good within the confines of a robust legal framework that protects Canadian values.

Consider this a call to action. Ontario's social and economic well-being requires a collective and sustained effort to understand the opportunities and challenges of data and unlock its potential.

SUMMARY OF RECOMMENDATIONS

A. RECOMMENDATIONS FOR GOVERNMENT

PRIVACY

RECOMMENDATION	ADDITIONAL RECOMMENDATIONS	GOVERNMENT ONTARIO	GOVERNMENT CANADA
Avoid duplicating federal government laws pertaining to the collection, use, and disclosure of personal information by private sector organizations.		●	
Preserve the principles-based nature of PIPEDA and PHIPA while encouraging the development and widespread adoption of industry standards or codes of practice.	• Facilitate the development of clear expectations around consent through a combination of legislative amendments to PHIPA and PIPEDA, clear guidance, and industry standards. • Build on international efforts to secure interoperability of privacy standards and ensure that Canadian authorities have immediate and complete access to information stored abroad for the purposes of investigation and enforcement. • Take a measured, industry-specific approach to data portability and allow sufficient time for businesses to implement any new requirements. • Continue promoting privacy by design as a best practice to help organizations comply with PIPEDA and PHIPA.	●	●
Take measured steps to strengthen enforcement of privacy laws while preserving the current ombudsman model. This may include giving the OPC limited order-making powers.			●
Experiment with small-scale civic data trusts.		●	

CYBERSECURITY

RECOMMENDATION	ADDITIONAL RECOMMENDATIONS	GOVERNMENT ONTARIO	GOVERNMENT CANADA
Encourage and monitor adoption of cybersecurity standards in sectors where they are not already enforced by regulators.	• Adopt globally recognized cybersecurity standards internally and within the broader public sector. • Work with industry groups to assess the strengths and weaknesses of cybersecurity defences across the economy and, where appropriate, help to address them.	●	●
Establish public-private partnerships focused on developing Ontario's cybersecurity talent pool and encouraging talent to remain in the province.	Continue to build pathways to data and digital literacy within the public education curriculum.	●	
Encourage municipalities to use provincial procurement vehicles for digital services when provincial cybersecurity standards are higher than municipal ones.		●	
Exchange information on an ongoing basis about public sector cybersecurity threats and defence techniques.	Owners of critical infrastructure should partner with the Canadian Centre for Cyber Security to share threat information and support the integration of cyber defence technology as appropriate and in a manner consistent with privacy obligations.	●	●

DATA SHARING

RECOMMENDATION	ADDITIONAL RECOMMENDATIONS	GOVERNMENT ONTARIO	GOVERNMENT CANADA
Work with organizations to clarify privacy and security expectations around data sharing in different sectors.		●	●
Continue transitioning towards a more centralized data management system for health care information.	Work with health care stakeholders to harmonize standards and technologies required to effectively share health data. This process could be informed by an arm's length stewardship committee.	●	
	Collaborate with federal and provincial counterparts to accelerate systemic, nationwide sharing of health data.	●	●
Improve upon both the speed and breadth of Ontario's open data system. Practices should include open contracting and proactive disclosures of completed freedom of information requests.	• Assist municipal governments in releasing a broader range of datasets by providing technical support, guidance around privacy and security, and information on the benefits for communities. • Establish a feedback loop with open data users to facilitate ongoing improvements to Ontario's open data catalogue.	●	

ARTIFICIAL INTELLIGENCE

RECOMMENDATION	ADDITIONAL RECOMMENDATIONS	GOVERNMENT ONTARIO	GOVERNMENT CANADA
Support commercialization and adoption of AI within Ontario.	• Implement the recommendations of the Expert Panel on Intellectual Property. • Leverage more innovation-oriented procurement processes to accelerate development of the AI marketplace.	●	
	• Continue to fund AI research, industry-academia partnerships, and implementation supports for businesses. • Target more support towards scale-up firms. • Harmonize federal and provincial innovation support programs. • Embrace a whole-of-government approach to streamline business supports.	●	●
Continue to work closely with industry to invest in regional internet network expansions and upgrades.		●	●
Partner with employers and training institutions across Ontario to support data and digital skills development.	Work with stakeholders to ensure diversity and inclusion are factored into workforce development initiatives.	●	
Carry out gap analyses to identify risks around AI and whether they are adequately addressed in current legal and regulatory frameworks. This review should take place on a recurring basis with support from stakeholder advisory committees.	• Based on the findings of a gap analysis, consider updating legislation and regulation to clarify protections against AI-related risks. Providing clarity around liability should be a priority. • Help ensure Canadian stakeholders are well represented and given a voice in international standard-setting forums. • Follow international best practices when procuring AI internally.	●	●

SUMMARY OF RECOMMENDATIONS

B. RECOMMENDATIONS FOR ORGANIZATIONS

CHAPTER	RECOMMENDATIONS	
Privacy	• Structure consent policies conscientiously to ensure customers are meaningfully informed of their options and empowered to exercise those options. • Exercise due diligence to ensure privacy and security requirements are met when transferring information to other jurisdictions.	• Facilitate data portability where doing so could have material benefits for consumers without unreasonably increasing risk. • Incorporate privacy by design across systems, where feasible, and keep up with the most up-to-date guidance and standards as they evolve. • Embrace transparency by openly communicating details about data privacy practices.
Cybersecurity	• Adopt and maintain best-in-class cybersecurity standards. • Share learnings and best practices to strengthen overall cybersecurity capacity within sectors and the wider economy. • Carry out comprehensive cybersecurity risk assessments and regard cybersecurity as a business risk rather than an IT risk. • Train staff regularly to build internal cyber hygiene.	• Where appropriate, adopt technology to help staff manage cyber threats. • Explore cybersecurity insurance options. • Industry owners of critical infrastructure should partner with the Canadian Centre for Cyber Security to share threat information and support the integration of cyber defence technology as appropriate and in a manner consistent with privacy obligations.
Data Sharing	• Businesses and research institutions should share data where possible while maintaining privacy and security, including through robust de-identification measures, and contribute to collaborative data sharing initiatives such as data libraries and the development of standards.	• Health stakeholders should support adoption of consistent standards around the sharing of health data.
Artificial Intelligence	• Work with international partners to advance and adopt responsible AI standards and best practices around risk assessments, transparency, and employee training. • Businesses that have not adopted AI should evaluate the applicability of AI to their own operations and experiment with its use.	• Take an active approach to upskilling workers with data and digital skills. A holistic approach should be taken to ensure employees across departments are equipped to work with or alongside AI.

ontchamberofcommerce

@OntarioCofC

company/ontario-chamber-of-commerce

www.occ.ca

ontario chamber of commerce

Indispensable Partner of Business

ISBN: 978-1-928052-67-8