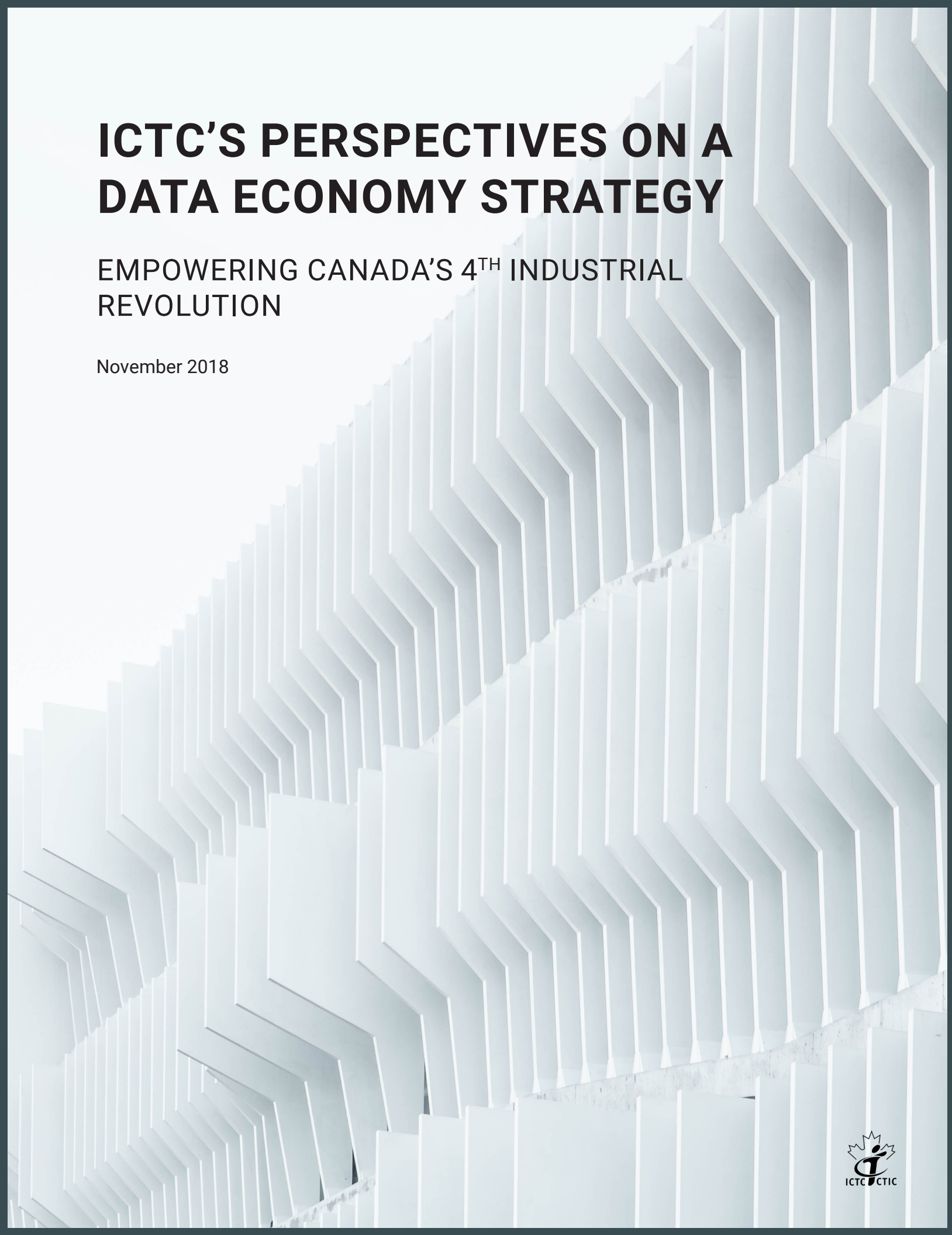
ICTC'S PERSPECTIVES ON A DATA ECONOMY STRATEGY

EMPOWERING CANADA'S 4TH INDUSTRIAL REVOLUTION

November 2018



Preface

As a not-for-profit, national center of expertise, ICTC strengthens Canada's digital advantage in a global economy. Through trusted research, practical policy advice, and creative capacity-building programs, ICTC fosters globally competitive Canadian industries enabled by innovative and diverse digital talent. In partnership with a vast network of industry leaders, academic partners, and policy makers from across Canada, ICTC has empowered a robust and inclusive digital economy for over 25 years.

To cite this paper:

Anani, N., Davidson, R. (November 2018), *ICTC's Perspectives on a Data Economy Strategy: Empowering Canada's 4th Industrial Revolution*, Information and Communications Technology Council (ICTC), Ottawa, Canada.

Cover image by Joel Filipe.

EXECUTIVE SUMMARY

This white paper highlights ICTC's response to ISED's Digital and Data Consultations in an era where a data-driven economy is a global stimulus for fledging entrepreneurs, and emerging industries to create and commercialize new Intellectual Property (IP) to achieve national, economic, and social aspirations.

Innovation: Canada's ability to fully partake in a global data-driven race will heavily depend on our ability as a nation to unleash open data innovations while maintaining public privacy, enhancing security, and enabling inclusive growth.

This will require a delicate balance between economic, democratic, and private interests that will govern the free flow of information across borders while maintaining Canada's comparative intellectual advantage in a global economy.

Canada's open data innovation landscape must be underpinned by a technology strategy that is built on API- enabled standards that empowers third party players to grow the ecosystem of applications and services to Canadians outside the confines of a vendor specific environment, in health, commerce, banking, transportation, and many others.

Privacy and Trust: Highly publicized data breaches and data privacy issues have eroded public confidence in both the private and public sectors' ability to responsibly collect, manage, and analyze their personal information. The environment created by the EU's General Data Protection Regulation (GDPR) has motivated Canada to review its own data and privacy legislation and ICTC recommends action is required to better address the areas of consent, data breach notification and enforcement mechanisms, and the importance of data portability rights.

The Future of Work: ICTC's labour market foresight points to the demand to fill 216,000 critical ICT positions by 2021, and job growth in ICT is outpacing the overall economy by 6 to 1. At the same time, non-digital jobs are being displaced by AI, robots, and other disruptive technologies. Comprehensive, national skills development initiatives are necessary to maintain and improve Canada's data and digital competitiveness.
ICTC asserts that carving a carefully designed "National Data Strategy" for Canada is an important impetus for signalling Canada's aspirations in this space and setting the stage for investment, growth, and social prosperity.

INTRODUCTION

With the increasing use and relevance of technology across all sectors of the economy, Digital+Data has evolved into a thriving, almost self-contained economy of its own. Just a few years ago, a major headline dubbed "data [as] the new oil", effectively identifying it as a virtual, endlessly renewable natural resource. Yet, with key developments in the digital realm like cloud computing, AI, 5G, augmented reality, IOT, blockchain and others, the very concept of data has been transformed. Data is now shaped into finished products (data brokers combining multiple data sources into powerful new products), into currency (cryptocurrencies) and into the fabric of civic governance (smart cities).

Increasing the use of data should not be the only goal as to reach its full potential, the Digital+Data economy requires a robust Open API ecosystem to streamline and institutionalize digital collaboration between all sector of the economy. Canada must also consider how it will protect Canadian IP in the Digital+Data economy and protect citizen's data rights similar to the EU's enforcement of the EU-US Privacy Shield. As the Digital+Data economy develops, Canadian competition regulatory bodies and lawmakers must ensure a healthy, competitive and innovative economy emerges. Net Neutrality protection is one such policy and regulatory issue to strengthen as inclusive growth will be the hallmark of a successful Canadian Digital+Data economy.

As the Digital+Data economy expands and accelerates, as do new governance challenges and considerations for governments and regulators. Headlines like Facebook's data usage and its links to Cambridge Analytica, the increase and sophistication of cyberattacks, and the general public's unease with Big Data all function to make data governance and regulation not only top of mind, but a central policy priority. The EU's General Data Protection Regulation (GDPR) (European Union, 2018) is a comprehensive if imperfect early move on the data protection front. While safeguarding the rights of users and their data is a cornerstone of the regulation, some aspects of GDPR are quite punitive to commercial entities. More, they do not only impact EU-based countries, but rather all countries who are engaged in business with EU states as well. Canada is especially impacted as the recent Canada-EU trade agreement, the Comprehensive Economic Trade Agreement (CETA), will necessitate GDPR compliance for many Canadian businesses. Understanding these requirements is a first step; designing policies that strike a balance between data regulation and promoting Digital+Data innovation is a must.

Canada's talent strategies, fiscal and financial, cultural, as well as competition policies will also need to respond to this new reality that is increasingly being termed as the new oil.

INNOVATION IN THE DATA AGE

There are many factors to consider when discussing Canadian innovation in the Digital+Data economy. The paramount consideration, however, is to be laser-focused on the segments of the Digital+Data economy that Canada can be sustainably competitive in. Spreading these resources too thinly and broadly may result in policies that are challenging to implement or ineffective.

AI

Canada possesses a significant window of opportunity when it comes to AI due to our existing leadership in the academic and research community. With the investments that competitors like China and the U.S. (Boyd, 2018) are pouring into AI and AI research however, this window risks becoming smaller the longer we wait. We can now benefit by selecting AI sectors, products and services that help us produce better and more competitive products than our international counterparts. Areas such as resource management, agriculture, food supply safety and government services are sectors where Canada has an international reputation of domain expertise.

Open Banking

Whereas AI is an area of strength for Canada, there are other notable segments of the Digital+Data economy where Canada currently trails woefully behind international counterparts. Open Banking is one such segment. Countries that have embraced Open Banking (enabling consumers to open their banking data to 3rd party service providers) (PWC UK, Open Data Institute, 2018) have had an industry pop up that offer these third-party services and builds the technologies to support them. While Canada is currently not supporting Open Banking directly, the 2018 Budget (Shecter, 2018) did include a recommendation to revisit and review this position.
The Open Banking movement is an example of data portability as an innovation engine, not just a privacy imperative. Industries including finance, telecommunications, healthcare, and transportation may all see increased service levels, with the potential for new supporting sectors to develop if data portability is embraced as an innovation catalyst.

Open API

In general, Canada is not an early adopter of transformational technologies. Open Banking is just one sector of the Open API movement. The Open API movement strives to increase the awareness and adoption of programmatic interfaces between applications in and, more powerfully, between organizations. Open APIs are what make data portability a sustainable and valuable service to citizens and consumers alike. The Open API movement, along with a complementary standards initiative, can accelerate innovation in the Digital+Data economy and help differentiate participant countries and organizations from more closed economies and corporations.

Digital+Data Economy Intellectual Property (IP):

As Canada develops its Digital+Data economy, there need to be protections in place for IP developed by Canadian companies. Europe is exploring a "sui generis data ownership right" to manage their data IP. The protections can be balanced with individual rights for data ownership and data portability, a one-size-fits-all approach to privacy and IP in the Digital+Data economy is not sustainable nor is it best for Canada. Canada can take a leadership role on IP by creating an IP Clearinghouse to enable easy access to multiple Canadian IP assets through standardized licensing and usage agreements.

Competition Policy

Another dimension to consider is the role of competition policy and the Competition Bureau of Canada in the success of the Canadian Digital+Data economy. Data monopolies and unbalanced market power distribution can only serve to hinder Canadian companies and consumers participation in the Digital+Data economy. Canada needs to develop a nation-wide geographic and sectoral competition policy to guide the development of an open and innovative Digital+Data economy.

Canada must also look at the Digital+Data economy through a net-neutrality lens and keep reinforce the need for a open and non-tiered data exchange environment to foster inclusivity, innovation and sustainability of growth for Canadian businesses.

Stimulate Private Investment in the Digital+Data Economy

If data is truly the "new oil", it is important to consider stimulus mechanisms used in traditional resource sectors to catalyze private sector investment in the Digital+Data economy. Instruments like flow-through shares and other tax incentives could expand the Digital+Data economy beyond a few well-established players and increase the viability of entrepreneurs into the market.

PRIVACY AND TRUST

Individual and vulnerable community information and data privacy is an ever-changing challenge. Advancements in personal devices, including the pervasive reach of social media into everyday lives and the rapid deployment of digital services in the public and private sector, only magnify the demand on public and private institutions to have robust, evolving privacy protections and best practices.

It is important for Canada to reconcile the gaps between the EU's GDPR and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) (Government of Canada, 2018), along with its provincial counterparts. The following represent key factors for consideration in this process.

Consent: PIPEDA possesses relatively strictly consent rules, whereas GDPR is more flexible. PIPEDA dictates consent as the *only* basis for collecting and processing personal data, whereas in the GDPR Article 6.1 there are six cases under which data can be legitimately processed, only one being via consent.

However, there is also much discussion and research concerning the appropriateness of consent-based models. Digital privacy philosopher Helen Nissenbaum (BERINATO, 2018) argues against the basic tenants of the digital/data consent model, citing "…misimpression of meaningful control …" and "…consent…it's simply not a measure of privacy…" as key reasons. Conversely, others like responsible data veteran Alix Dunn (Anna Scott, 2018) proposes agile ethics as a model to integrate into privacy models. Alix Dunn defines agile ethics as "The purpose of 'agile ethics' is to facilitate working ethically at speed, and it is a practice that can be designed to operate in tandem with agile development." (Dunn, 2018)

The recent headlines concerning Statistics Canada requesting personal banking information from financial institutions, have drawn attention to the Statistics Act. Teresa Scassa, a University of Ottawa professor who specializes in information law, highlighted the issues with the broad use of the Statistics Act in the digital age:

> *"It was drafted in an analogue age. It's talking about the requirement of organizations to provide documents and records," she said. "They've just read it as now including digital documents or records."*
>
> *"The analogue world had inherent limitations on what could be achieved by something like this. I mean, there is only so much paper you could transfer," she said. "Data breaches are a significant and realistic concern." (Russell, 2018)*

Navigating this environment necessitates the development of clear frameworks that identify appropriate responses. Canadians need a national data consent legislative framework to not only protect their rights, but to disambiguate the differences between PIPEDA and provincial privacy regulations – some of which can be challenging to compartmentalize. The consent framework should also be tiered based on the relative and potential risks associated with the specific categories of personal data (consumer, health,

location, religion, politics, etc.), to whether the data is necessary for delivering the specific service/product to the individual, and to whether or not the consent request can be truly considered informed consent based on appropriate standards or benchmarks.

Data Breaches: PIPEDA and the Digital Privacy Act (Canadian Government, 2018) provide a framework that requires data breaches to be reported to the Canadian Privacy Commissioner along with the individuals impacted, when the breach possesses a real risk of harm. By contrast, GDPR does contain strict breach protocols and associated administrative fines for non-compliance (which can be significant), but it does not require the same level of individual notification as PIPEDA. Making the Digital Privacy Act a living, agile legislation that can be quickly updated to keep up with the ever-changing landscape of technology, cyber threats, and Canadians' privacy demands, would help Canada can better prepare for and respond to cyber challenges.

In addition to this, coordinated efforts between law enforcement, intelligence, cyber security agencies, and organizations managing data digitally is key. With cyber threats and attacks becoming more widespread and prevalent, more and more it is not a matter of *if* an organization is going to be breached, but *when*. This collaborative coordination can start with awareness, education and breach response protocols. For example, it may not always be desirable to hit the kill switch on a breach before coordinating with law enforcement and other agencies. In fact, oftentimes, these agencies may need the breach to remain open in order to see if attackers and the true intent of the attack – for example, ransom attacks acting as diversions to more extensive attacks - can be identified.

Lastly, Canada should develop a data breach enforcement mechanism. Failing to do so may result in adverse effects when it comes to breaches, such as companies downplaying the scale or impact. A regulatory entity in Canada that can handle complaints and even perform spot audits on the various breaches reported from time to time, and where necessary, fine companies is essential. Models to consider include the North American Electric Reliability Corporation (NERC) (NERC, n.d.) and the CRTC complaints mechanism.

Data Portability: GDPR requires data portability for individuals. This is potentially the most impactful requirement for Canadian organizations. Article 20 (European Union, 2018) requires organizations to provide individuals the data they hold about them in a structured, machine-readable format, allowing them to manage it themselves and/or take it to another service provider. PIPEDA does not require data portability. While some Canadian organizations may initially struggle with this requirement, ultimately Canadians should have the right to shut-down their account with one company and port their data elsewhere. An important byproduct of a policy like this is in relation to the spurring of competition among service-providers. Essentially, data portability can urge companies to compete for individuals' data and business, in the interest of not losing access to valuable information under an environment where data is money. Using the GDPR provisions as a starting point, Canada should create a regulatory mechanism to require data portability.

The Right to be Forgotten: There is an argument to be made that in instances where Canadians feel their personal data has been altered, misused, or otherwise negatively impacted, they should have the right to have it lawfully erased. The ability to have personal

data erased from a data controller (Google, Facebook, etc.) is, however, a complicated concept. It runs up against the First Amendment in the U.S. (Abrams, 2018). and could be abused by politicians, business people and criminals to coverup past activities and deeds the public should have the right to know about. The GDPR has outlined when the Right to Be Forgotten (European Union, 2018) can be applied and enforced, whereas current Canadian legislation contains no Right to be Forgotten provisions. What is clear is that a one-size-fits-all approach to the Right to be Forgotten is neither feasible or appropriate. One example where a blanket approach would not be appropriate could be in cases involving minors. Here, a regulatory framework that would enable the Right to be Forgotten for youth below the age of 18 should be considered, where for non-minors it may not always be reasonable. An initial Senate investigation into the appropriateness of the Right to be Forgotten under the Canadian context would be a welcome first step.

Employee Data: The GDPR (European Union, 2018) contains broad requirements for the collection and the processing of employee data. Conversely, PIPEDA only applies to a small group of federally-regulated employers. All other employers are regulated provincially, and only a select number of provinces enforce specific employee data privacy considerations. The problems related to this inconsistency of regulation is something that may be further exacerbated with the rise of the gig economy - something that extends beyond national, let alone provincial borders, and makes it harder and harder to clearly define who is or should be considered an "employee". Canada should to move quickly to harmonize federal and provincial employee data privacy laws, and to educate the private sector on the implications of GDPR compliance to employee data regulations under GDPR.

Digital+Data – the good and the bad – does not respect traditional borders. And ultimately, the spread and adaption of digital technology is dependent on user acceptance and trust. Canada can take a leadership role in the data privacy and trust space by championing an international collaborative and adaptable privacy/trust framework detailing standards for data commercial and public data use. Any initiative to forward this agenda must also be integrated with the Canadian Centre for Cyber Security. Selecting best practices and technology/data standards must be a cross-government initiative, supplemented by collaboration with our international partners.

A first step could involve a collaboration between Canada, the UK, New Zealand and other d7 partners on GDPR compliance and the improvement and integration of PIPEDA and its provincial counterparts. This should all be done in the interest of protecting Canadians' data rights while supporting a market approach to Digital+Data regulation. At the same time, Canada's collaboration with its 5 Eyes partners on cybersecurity can lead to more robust, hardened protections for Canada's privacy infrastructure. This, in turn, can help reinforce and rebuild Canadians' trust of government privacy capabilities.

The recently signed USMCA has a chapter on Digital Trade (US, Mexico, Canada) and directs the parties to consider the principles and guidelines of APEC and the OECD. The U.S. also deals with the EU-US Privacy Shield but with the EU reviewing PIPEDA for adequacy under GDPR over the next four years, Canada needs to be proactive to insulate Canadian Digital+Data economy participants from adverse regulatory, treaty, and/or compliance impacts.

The importance of trust cannot be understated. The 2018 Edelman Trust Barometer (Edelman, 2018)shows a trust challenge in Canada when it comes to governments, businesses, and media. While the survey was conducted and results were released prior to recent developments like the Facebook/Cambridge Analytica story, it showcases the underlying concerns that many Canadians may possess when it comes to trusting various institutions with their data. The Canadian government should work with the private sector and civil society to help shape an information ecosystem that can be trusted, embraced, and leveraged by Canadians for innovation and social good.

Open data is a foundational element of a trust rebuilding framework. Open data can enable civil society organizations (NGOs, charities, non-profits) to better serve Canadians and provide businesses opportunities to innovate and develop new products and services. Open contracting data, in particular, can open up government procurement opportunities to domestic small to medium-sized businesses (SMBs), increasing their competitive resilience and help fund their innovation and growth.

FUTURE OF WORK

Canada is facing a 216,000 digital worker shortfall by 2021 (McConnell, 2018). At the same time, there are real concerns about how the Digital+Data economy may displace some non-digital jobs. When it comes to a holistic approach to the challenge of displacement, Canada is at a bit of a disadvantage too in comparison to some of its peers, as education is primarily a provincial jurisdiction. This potential mismatch across the provinces can result in difficulty when it comes to the development of comprehensive responses to national skill shortfalls.

Canada, like many countries, also has difficulties engaging youth in the Science Technology Engineering, and Mathematics disciplines. This challenge is often compounded for women and Indigenous peoples, who continue to be underrepresented in STEM and digital fields. Inclusion, diversity and accessibility must be at the pinnacle of our digital agenda.

Opportunity

One area where Canada can show leadership, however, in is the building of a robust and trusted micro-credentialing ecosystem. As leading businesses like IBM, Google and Apple begin to shift away from the need for traditional post-secondary degrees for employees (Connley, 2018), the world is also moving away from traditional modes of credentials and professional designations. Online, on-demand courses are often filling the gap for existing and prospective digital workers that need to reskill or upskill to meet industry demands, yet there are very few mechanisms to verify and endorse course content or the veracity of a participant skill levels. This type of componentized credential obtainment is called micro-credentialing. Canada can take a giant step forward by working with the private sector, non-profits and traditional credential management organizations like the Chartered Professional Accountants of Canada and Engineers Canada to build a viable and trusted micro-credentialing platform.

The benefits of doing so are immense. Micro-credentialing can help existing workers stay up to date with skill needs, and it can enable the transition of workers from other sectors into the digital space. However, the benefits don't end there. Micro-credentialing can also lower digital entry barriers for indigenous peoples in both remote and urban settings, helping them develop competitive digital skills. Micro-credentialing can also can be a benefit to peoples with disabilities, who may want to participate in the Digital+Data economy, but is unsure of appropriate pathways to do so. Lastly, as the government and industry experiment with gig-like hiring through initiatives like TalentCloud (Canada School of Public Service, 2018), the ability to verify a candidate's skill credentials will become more pressing and relevant. Adopting an early framework by which to do so will give Canadian-based companies a distinct advantage in the international Digital-Data economy.

Challenge

One of the major data challenges facing the Canadian government is the availability of reliable and granular data, essential to the development of an accurate Digital+Data

economy Labour Market Information (LMI) system. Statistics Canada currently provides monthly labour market survey results (Statistics Canada, 2018), under the following coding schemes:

- National Occupation Classification (NOC) codes
- North American Industry Classification System (NAICS) codes

However, while useful for showcasing a broad picture of historical labour and industry trends at a macro level, at times these categorizations can be too outdated and too high-level to use for accurate and forward-looking Digital+Data economic planning and promotion. There is a strong need for a more flexible and adaptable coding framework that would enable the analysis of specific trends such as high-growth subindustries like Advanced Manufacturing or Autonomous systems, or in-demand sub-occupations like data analysts or cybersecurity specialists. This would allow the Canadian government to better plan economic initiatives and effectively promote Canada as a destination for specific Digital+Data international investments. The EU has been piloting a framework called the European Skills, Competences, Qualifications and Occupations (ESCO) (Extending ESCO, 2018). One of the core components of this pilot is the extensibility of the classification system:

> *"…In order to achieve a deeper level of detail in ESCO, e.g. for specific economic sectors, the occupation and skill pillars of ESCO can be extended. This is useful for building sector-specific applications of higher accuracy, e.g. job-matching, workforce planning or career guidance tools for a specific economic sector." (European Commission, 2018)*

This extensibility for the Digital+Data economic sector would prove invaluable for Canadian governments and businesses under the right framework.

ADDITIONAL PRIVACY/INNOVATION OPPORTUNITIES

There are some advantages to the PIPEDA + Digital Privacy Act and some disadvantages when compared to GDPR. One core aspect of GDPR is placing much of the management of data privacy on the individual – something that in many ways leaves compliance with the individual, which can be onerous for many to stay abreast with A particularly relevant concept to reduce the burden of data management on the individual is that of Data Representatives. The role is akin to a digital personal assistant crossed with a lawyer service that can be offered to individuals, meaning that they will not have to be cognizant of all the regulations and data exposures we all have. A non-digital economy analogue would be tax attorneys, only this service would be digital, free of cost, and behind the scenes. That said, the development and standardization of this role would need to be developed with certification authorities, professional associations and government oversight. This is one area where Canada has an opportunity to take in the lead. This is something that can lead to growth in and export products and services that support this new digital industry.

Another opportunity takes the form of data trusts. Canada can get ahead of some of the obstacles in the Digital+Data economy by establishing a governance framework for data trusts instead of waiting for a patchwork of disparate data trust rules to develop organically. Data trusts are mechanisms that can establish ground rules for accessing and processing collections of data. As an example, a smart city project may establish a data trust to protect the city and the public's right to have access to the data the smart city platform collects. Data trusts can also be structured to foster innovation by establishing governance rules for datasets accessible to industry startups and established players. With the rise of smart cities and smart city features like connected grids, this should be a component to all related procurement processes.

SUMMARY OF POLICY RECOMMENDATIONS

Innovation:

1. Embrace data portability regulation not just as a privacy issue, but as an engine for innovation. Open Banking is clear first step, but every industry can be benefit from and become more competitively resilient domestically and internationally through data portability. This will require legislative action to entrench data portability rights and regulatory support and enforcement.
2. Federal programs to incent the creation and deployment of Open API initiatives to build a healthy and growing Digital+Data economy.
3. Develop IP protection policy and infrastructure that supports the principles of the Digital+Data economy.
4. Create a federal competition policy framework that keeps the digital and data companies in Canada succeeding in a healthy and competitive market.
5. Embark on a stimulus initiative to include more Canadian businesses and entrepreneurs into the Digital+Data economy.
6. Take a leadership role in the creation of a Data Representative framework, and develop, market and export products and services to support this new digital industry.
7. Establish a federal governance framework for data trusts.

Privacy and Trust:

1. The development of a national data consent legislative framework to protect individual rights when it comes to personal data collection and use, and to disambiguate the differences between PIPEDA and provincial privacy regulations.
2. The revision of the Digital Privacy Act, making it a living, agile legislation via regulatory mechanisms that can be quickly updated to keep up with the ever-changing landscape of technology, cyber threats, and Canadians' privacy demand.
3. The creation of a multi-stakeholder data breach preparation and response team; a coordinated effort between law enforcement, intelligence, cyber security agencies, and organizations managing data digitally.
4. The establishment of a regulatory entity in Canada that would handle data breach complaints and perform spot audits on various breaches reported. This entity must have enforcement and punitive measure powers to discourage insufficient data protections. This institution needs to have a rapid response protocol for large-scale and strategically detrimental breaches.
5. The creation of a regulatory body tasked with:
    a. The development, implementation, and management of national data privacy standards.
    b. The promotion and enforcement of data portability regulations. Canadians should have the right to shut down their account with one company and port their data elsewhere.
    c. Enabling and streamlining the Right to be Forgotten for youth below the age of 18, with appropriate responses for those over 18 to be determined on a case-by-case basis.

d. Harmonizing federal and provincial employee data privacy laws. This should be coupled with tactical and industry-specific education campaigns for the private sector on the implications of GDPR compliance to employee data regulations under GDPR.

The Future of Work and LMI:

1. Develop a flexible framework by which to timely and accurately capture employment and industry realities under the NOC and NAIC system. Doing so would enable the capturing of new developments in the digital economy, both in terms of up and coming sectors, as well as in-demand occupations. Relevant amendment processes could involve the separation of sub-industries and sub-occupations from the broader NAIC and NOC group for added granularity. The Canadian government and the private sector need better, more granular LMI trends data to support the private sector with sector-specific policies and compete internationally for Foreign Direct Investment.
2. Address data suppression challenges related to the NAIC and NOC systems in a way that provides more valuable, accurate and granular-level data, while taking data protection and privacy needs into account. One potential solution may be lowering the data suppression level from its current 1,500 sample to at least 1000. At a 1000 suppression level, this would not only allow for the showcasing of reliable data at the regional and city level – something increasingly important as we move towards smart city conceptualization – but would also be more closely aligned with data suppression standards of leading organizations like the OECD. Alternatively, allowing for the access of microdata for specific statistical research purposes (for example, providing aggregated accurate employment forecasts at a city or regional level) may also be an option.
3. Take a global leadership role in the future of work in the Digital+Data economy by working with the private sector, non-profits and traditional credential management organizations like the Chartered Professional Accountants Canada and Engineers Canada to build a viable and trusted micro-credentialing platform.

WORKS CITED

Abrams, F. (2018, 05 7). *When 2 + 2 Might Equal 5*. Retrieved from The New York Times: https://www.nytimes.com/2018/05/07/opinion/google-right-to-be-forgotten-first-amendment.html

Anna Scott, A. D. (2018, 10 05). *'agile ethics', how innovative organisations can adopt them and why diversity is so important to ethics*. Retrieved from Open Data Institute: https://theodi.org/article/agile-ethics-pioneer-alix-dunn-on-how-to-minimise-harm-and-why-moving-fast-and-breaking-things-must-not-extend-to-ethics/

BERINATO, S. (2018). STOP THINKING ABOUT CONSENT: IT ISN'T POSSIBLE AND IT ISN'T RIGHT. *Harvard Business Review*. Retrieved from Harvard Business Review: https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right

Boyd, A. (2018, 10 9). *East vs West in a race for AI supremacy*. Retrieved from Asia Times: http://www.atimes.com/article/east-vs-west-in-a-race-for-ai-supremacy/

Canada School of Public Service. (2018, 09 12). *The GC Talent Cloud*. Retrieved from Canada School of Public Service: https://www.csps-efpc.gc.ca/events/gctc/index-eng.aspx

Canadian Government. (2018, October 10). *Digital Privacy Act*. Retrieved from Justice Laws Website: http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2015_32/page-1.html

Connley, C. (2018, 10 8). *Google, Apple and 12 other companies that no longer require employees to have a college degree*. Retrieved from CNBC: https://www.cnbc.com/2018/08/16/15-companies-that-no-longer-require-employees-to-have-a-college-degree.html?__source=facebook%7Cmain

Dunn, A. (2018, May 7). *Working Ethically At Speed*. Retrieved from Medium: https://medium.com/@alixtrot/working-ethically-at-speed-4534358e7eed

Edelman. (2018). *The 2018 Edelman Trust Barometer.* New York: Edelman.

ENCQOR. (2018, 10 10). *ENCQOR*. Retrieved from ENCQOR: https://www.encqor.ca/

Eric Auchard, S. N. (2018, 03 15). *What is 5G and who are the major players?* Retrieved from Reuters: https://www.reuters.com/article/us-qualcomm-m-a-broadcom-5g/what-is-5g-and-who-are-the-major-players-idUSKCN1GR1IN

European Commission. (2018, 10 10). *Extending ESCO*. Retrieved from European Commission: https://ec.europa.eu/esco/portal/escopedia/Extending_ESCO

European Union. (2018, October 10). Retrieved from EUR-Lex - Access to European Union law: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN

Extending ESCO. (2018, 10 10). *Extending ESCO*. Retrieved from European Skills, Competences, Qualifications and Occupations: https://ec.europa.eu/esco/portal

Government of Canada. (2018, October 10). *The Personal Information Protection and Electronic Documents Act (PIPEDA).* Retrieved from Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

McConnell, J. (2018, 01 31). *The digital economy has created a demand for 216,000 more tech workers, report finds*. Retrieved from Financial Post: https://business.financialpost.com/technology/the-digital-economy-has-created-a-demand-for-216000-more-tech-workers-report-finds

NERC. (n.d.). *Home Page*. Retrieved from North American Electric Reliability Corporation : https://www.nerc.com/Pages/default.aspx

PWC UK, Open Data Institute. (2018, 10 10). *The future of banking is open*. Retrieved from pwc uk: https://www.pwc.co.uk/openbanking

Shecter, B. (2018, 02 27). *Federal budget: Ottawa to study merits of 'open banking,' a catalyst for fintech*. Retrieved from Financial Post: https://business.financialpost.com/news/fp-street/ottawa-to-study-merits-of-open-banking-a-catalyst-for-fintech

Statistics Canada. (2018, 10 10). *Labour Force Survey*. Retrieved from Statistics Canada: https://www.statcan.gc.ca/eng/survey/household/3701#a2

The Canadian Press. (2018, 09 28). *Internet groups disappointed in lowered CRTC speed minimums for broadband fund*. Retrieved from Financial Post: https://business.financialpost.com/pmn/business-pmn/internet-groups-disappointed-in-lowered-crtc-speed-minimums-for-broadband-fund

US, Mexico, Canada. (n.d.). *Chapter 19: Digital Trade.* Retrieved from Office of the U.S. Trade Representative.