STANDARDS RESEARCH

The Digital Age: Exploring the Role of Standards for Data Governance, Artificial Intelligence and Emerging Platforms

May 2019

Authors

Kiran Alwani, Mowat Center

Michael Crawford Urban, Mowat Center

Advisory Panel

Howard J. Deane, Consumers Council of Canada

Jay Jackson, Consumers Council of Canada

Laurie Amiruddin, CSA Group

Nancy Bestic, CSA Group

Helene Vaillancourt, CSA Group

Namat Elkouche, CSA Group (Project Manager)

Contents

Executive Summary

In recent years, digital technologies have become increasingly ubiquitous in our everyday lives. These technologies have transformed the way we socialize, shop, work and entertain ourselves. In terms of its economic implications, the digital economy currently facilitates billions of connections daily to enable business activities and transactions transnationally that were previous impossible due to geographical distance, logistical inefficiency or political barriers.

In particular, digitization has led to the creation of vast new quantities of data, which can be used to create new products and services, as well as train artificial intelligence (AI) algorithms to make important decisions or influence people's behaviours. Many types of digital platforms have also become widespread, with many serving as marketplaces for goods and services, and as intermediaries that match workers to clients or consumers.

While such advancements have increased convenience and efficiency, the growing pervasiveness of the digital realm and its encroachment on activities previously conducted in person or by humans have also raised a host of novel concerns. "Surveillance capitalism" business models have reduced privacy and security for people by monitoring their online activities and commodifying their data. Algorithms used to influence behaviours or make important decisions are raising alarming ethical concerns. Skewed digital platform business models and their all-encompassing Terms of Service (ToS) agreements have led to a handful of powerful companies monopolizing many important areas – often usurping powers previously monopolized by governments.

In this context, where traditional laws and regulations are all-to-often proving inadequate, it is obvious that there is need for new forms of governance that can effectively address these novel challenges. Standards development organizations (SDOs) have the opportunity to play an important role due to their credibility, international connections and ability to bring together expertise from diverse sectors. Moreover, in addition to developing standards-based solutions to the pressing problems that have accompanied the rise of the digital economy, these new challenges also provide SDOs with the opportunity to modernize their processes for the digital age.

This report discusses three important areas of the digital economy and the opportunity for standards-based solutions in each:

Data governance: The widespread use of data has raised concerns around its collection, use and protection. In particular, concerns around privacy and security of citizens' data and informed consent have become widespread. Regulations such as the EU's General Data Protection Regulation (GDPR) have emerged in response, and standards have the potential to identify best practices in its implementation and assist organizations in demonstrating compliance through certification. Additionally, there is potential to create new standards for ToS agreements to promote informed consent and reduce power imbalances between users and firms. Furthermore, there is also great demand for standardization of data. SDOs have already developed some data standards and are developing more. Nonetheless, there remains significant scope for more work to meet this growing demand. Finally, there is also potential for innovative new thinking around how traditional SDOs can do better to match the rapid pace of change in the digital sphere, and leverage technology via machine readable standards or digital compliance registries.

Algorithms and AI: The use of algorithms for decision-making is spreading across sectors, including areas such as immigration application processing, predictive policing and the pricing of goods and services online. These algorithms have often come under fire for perpetuating existing societal biases such as racism and not being inclusive towards those at the margins of the society such as people with accessibility needs. This is particularly alarming since these critical decisions can deeply affect individuals' lives, particularly individuals from marginalized groups, in detrimental ways. Governing AI and other forms of algorithmic decision-making is particularly complex due to their "black box" character – many times, even the creators cannot understand how an algorithm reached its decision. SDOs can contribute to improving governance in this difficult area by creating data standards for training of AI, and developing tools or incubators to test algorithmic behaviour.

Digital platforms: In many sectors of the economy, digital platforms have reduced transaction costs, facilitated connections and increased flexibility and opportunity. At the same time, they have led to decreased competition, the concentration of power amongst a handful of global players and facilitated the exploitation of workers on digital labour platforms. An important reason for these issues is that platforms are often designed in ways that favour platform operators at the expense of users. Due to their international presence, credibility and access to expertise, SDOs are well-positioned to work towards creating standards for platform architecture and ToS to reduce power imbalances, promote interoperability and increase competition. In addition, SDOs can pioneer the development of a framework for digital labour rights addressing areas such as compensation, benefits, performance evaluation and dispute resolution.

1 Introduction

In the past 20 years, a series of new digital technologies, and the business models that they enable, have come to dominate much of the economy. This shift has created a host of novel challenges in areas as diverse as competition, privacy and labour rights. In response, there is growing consensus across society that the current under-governed character of these digital spaces needs to change.

But even as the need for more effective governance grows, change will not be easy. Building governance mechanisms for the digital economy is a project that faces many obstacles. Most obviously, the global scope of digital technologies transcends traditional jurisdictional boundaries, making action at the national level difficult to sustain. Moreover, these challenges will only grow more acute as the emergence of even more powerful and novel technologies continues.

Is there a role for standards-based solutions to help address these challenges? This report provides responses to this question with regards to three critical parts of the digital economy:

- **Data governance:** The emergence of "surveillance capitalism," a digital business model focused on the collection and exploitation of users' data, has raised many concerns (Zuboff, 2015). Specifically, security breaches like those at Equifax and Yahoo, and scandals like Facebook's links to Cambridge Analytica, have raised questions regarding informed consent, data security, privacy, accountability and the ethical use of user data.
- **Artificial intelligence (AI) and algorithms:** The use of AI and algorithms is spreading through society and the economy and replacing human actors in contexts as diverse as judicial sentencing, employee scheduling and the generation of consumer recommendations. The bases for algorithmic decisions often lack transparency, making it difficult to evaluate decisions' alignment with human rights codes, labour laws or other governance frameworks. Digital firms are also increasingly using algorithms to set prices based on inputs such as a user's postal code and their browsing history and in ways that may be undermining economic fairness.
- **Digital platforms:** The structural characteristics of digital platforms have helped to make these platforms useful and central to the digital economy. But these characteristics have also created significant power imbalances between platforms and different types of users. This is particularly so in cases where digital labour platforms serve as marketplaces for matching workers (e.g. drivers, hosts and freelancers) to consumers/clients. While they offer workers flexibility and new opportunities to earn income, the lack of labour standards governing these platforms means that work in the resulting "gig economy" is often unsafe and precarious.

This report begins by defining and describing the digital economy. This includes highlighting the opportunities and challenges that its emergence has unleashed, especially in the Canadian context. This section also includes a brief introduction to standards-based solutions and exploration of their potential uses in this emerging space.

Next, the analysis shifts gears and focuses on the potential roles for standards-based solutions in each of the report's three areas of focus. The examination of each area comprises two subsections. For data governance, this includes subsections focused on data collection and use and data security, while the AI and algorithms section is subdivided into algorithmic decision-making and algorithmic pricing. The digital platforms section is split into examinations of structural issues and digital labour platforms.

Each subsection begins with a survey of applicable existing and emerging governance instruments. This is followed by a discussion of the most important challenges currently impacting each area. The final part is devoted to an analysis of the opportunities that exist for standards-based solutions to help address some of the challenges identified earlier.

The report closes with a series of recommendations. These recommendations, which are directed at governments, regulators and standards development organizations (SDOs), highlight possible standards-based solutions to some of the critical challenges facing the digital economy, especially in the Canadian context.

Methodology

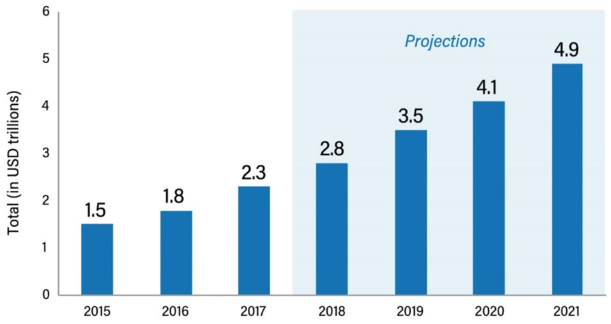
This report is the result of a mixed research approach. It builds on previous research conducted by the authors for other projects focused on topics including the sharing economy, blockchain technology and digital competition. This research was supplemented by original research for this report that included reviews of academic and grey literature such as news reports. Most importantly, it also included a series of 16 confidential semi-structured key informant interviews conducted with individuals from a variety of relevant fields ranging from technology entrepreneurs, to advocates for people living with disabilities, to academics, to policymakers, to standards, privacy and cybersecurity experts. These interviews were conducted either in person, by phone or by email.

2 Setting the stage

Digital technologies have transformed the global economic landscape by changing how consumers and businesses interact, how services are provided and how value is created. These changes are rapidly undermining the viability of many traditional business models.

While there is no universal definition, one way of defining the digital economy is to see it as "economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes" (Cassar, Heath, and Micallef). Mobile Internet, the Internet of Things (IoT), cloud computing, robotics and digital platforms are all technologies that are fostering more, and more impactful, digital connections. These connections are not merely local, but are allowing people to engage in the global economy without many of the constraints previously imposed by geography or political boundaries.

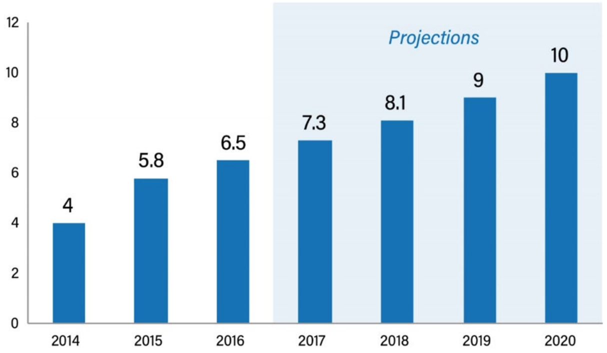
***Figure 1 –** Retail e-commerce sales worldwide from 2014 to 2021 (in trillion U.S. dollars)*



Source: (Statista, 2019a).

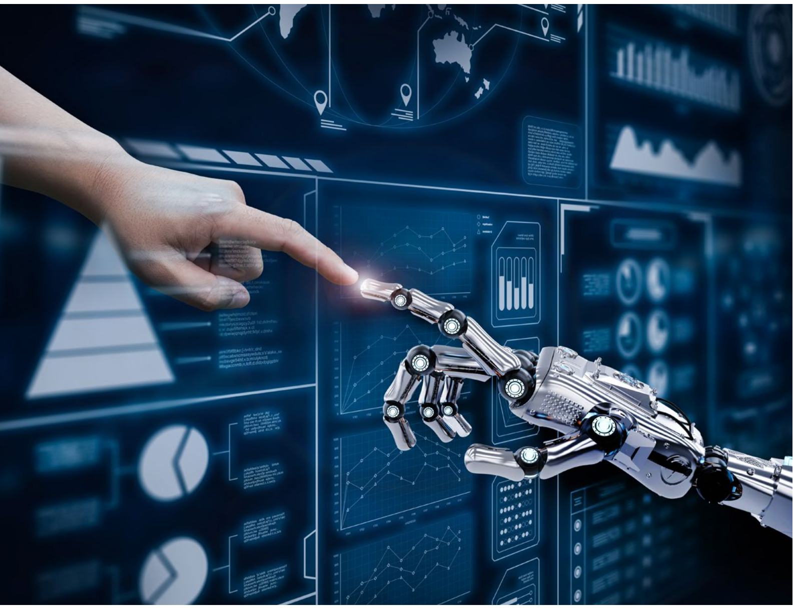
While e-commerce is likely the part of the digital economy most familiar to Canadians (see Figures 1 and 2), it is by no means the only part of the economy being impacted by the digital revolution.

***Figure 2 –** E-commerce as percentage of total retail sales in Canada from 2013 to 2020*



Source: (Statista, 2019b).

The digital economy is more than just e-commerce and includes other important sectors where digital technology plays a role. The Canadian information and communications technology (ICT) sector, which accounted for $43 billion, or three per cent, of Canada's GDP in 2016, is one good example (Canada's Economic Strategy Tables, p.2). But even adding technological sectors fails to capture the true scope of the digital economy as many "traditional" firms have integrated digital technologies like email and Internet-enabled



"In reality, the digital economy has already spread throughout much of the rest of the economy."

credit card payments into their businesses. In reality, the digital economy has already spread throughout much of the rest of the economy.

Digital economic activity is growing rapidly. According to a survey conducted between July 2017 and June 2018, 76 per cent of Canadians use a debit card, credit card, online banking or pre-authorized transactions for most of their personal spending. And from November 2015 to October 2016, about 2 million Canadians used app-based ride-sourcing services like Uber or Lyft, and spent about $240.8 million doing so (Statistics Canada, 2017). From July 2017 to June 2018, 28 per cent of Canadians made money through online platforms (Statistics Canada, 2018).

2.1. Opportunities and challenges – an overview

The emergence of new digital technologies has created both enormous new opportunities for individuals and significant and worrying challenges. And data lies at the heart of both.

The digitization of the economy involves the creation of vast new quantities of data, the analysis and extraction of valuable insights from this data and the use of these insights to create new tools, products and services. Indeed, in 2017, *The Economist* magazine declared data the world's most valuable resource (6 May, 2017). Given the importance of data, policymakers and civil society stakeholders are increasingly focused on answering numerous, and increasingly complex, data-related questions such as: How should citizens' data be stored, used and shared? How should privacy be safeguarded? What is involved in meaningfully consenting in an informed way to the use of one's data?

Data's importance is made particularly clear through its connection to what will be one of the most significant technological developments ever: AI. While AI algorithms are already common – the recommendation algorithms used by firms like Netflix and Spotify are well-known examples (Safian, 2018) – the truly transformative benefits of AI, such as its ability to help discover new pharmaceuticals (Fleming, 2018), still lie in the future. But to unlock these exciting prospects, AI will need access to vast quantities of training data.

Canada is well-placed to be at the forefront of AI development with Montreal, Toronto and Kitchener-Waterloo already counted as globally important research hubs. The Government of Canada has also invested $125 million to create a Pan-Canadian Artificial Intelligence Strategy and has picked an AI project (SCALE AI) as one of its innovation "superclusters."[1]

Nevertheless, to seize the opportunities presented by AI and "Big Data," significant challenges must be overcome. For instance, concerns regarding consent and

[1] The Innovation Superclusters Initiative challenged "Canadian businesses of all sizes to collaborate with other innovation actors, including post-secondary and research institutions, to propose bold and ambitious strategies that would transform regional economies and develop job-creating superclusters of innovation, like Silicon Valley". See https://www.canada.ca/en/innovation-science-economic-development/news/2018/02/government_of_canadasnewinnovationprogramexpectedtocreatetensoft.html

privacy in the new data-driven economy are gathering intensity. Indeed, in November 2018, Canada's Privacy Commissioner wrote to the Minister of Innovation stating that:

> *Recent events have shed light on how personal information can be manipulated and used in unintended, even nefarious, ways. I am growing increasingly troubled that longstanding privacy rights and values in Canada are not being given equal importance within a new digital ecosystem eagerly focused on embracing and leveraging data for various purposes. Individual privacy is not a right we simply trade away for innovation, efficiency or commercial gain (Privacy Commissioner of Canada, 23 November, 2018).*

Finally, while AI and data-related concerns grab the headlines, digital platforms also remain controversial and continue to reshape many parts of the economic landscape. For example, while digital labour platforms have made it easier for individuals to access work and provided many workers with valuable employment flexibility, the rise of these platforms has also raised concerns over their potential contribution to increased precarity and the undermining of legal and regulatory frameworks designed to protect workers.

2.2. What are standards and why are they important?

Broadly speaking, standards are instruments that set out "rules, guidelines or characteristics for activities or their results" (Standards Council of Canada). Standards first became important during the Industrial Revolution when long-distance trade and rapid industrialization created the need for reliably similar machine parts. These standards, often voluntary but sometimes legally mandated, have become critical to increasing safety and economic efficiency (Ditta et al. 2017, p. 12). They are also vital in fostering competition, for example, by promoting industrial interoperability (Girard 2019, p. 2).

Conformity to standards is generally assessed through testing, certification and inspection. Certification allows consumers to be more confident in their product choices, gives firms a competitive edge and assists regulators in ensuring that standards for important product features, such as health and safety, are met.

Nevertheless, traditional SDOs face challenges as they seek to update their processes for the digital age. One of the most prominent challenges is that the deliberative processes associated with traditional standards development, which are important for ensuring quality and incorporating stakeholder input, line up awkwardly with the speed of digital innovation. Additionally, since market power in the digital economy is increasingly concentrated in a handful of large firms, cooperation from these firms takes on outsized importance. Consequently, these firms often possess the ability to frustrate standards-setting initiatives which they oppose.

3 Data governance

The idea that data has dethroned oil as the world's most valuable resource has become a commonplace. "Big Data," the name given to both the pools of data of unprecedented size that have accumulated in recent years and the growing ability to analyze this data using computers, is becoming a major consideration in decision-making in industry and at all levels of government.

Big Data holds much promise, but its emergence also poses important challenges in areas like privacy, security and the inequitable distribution of its benefits. While much of Big Data's impact is still to be determined, it is already clear that the rules which govern data are in need of renewal. This section explores the potential for standards-based solutions to play a role in this renewal with an emphasis on two main areas of activity: data collection and usage, and data security.

As will be the case for all three substantive sections of this report, analysis of each area of activity begins with an examination of applicable existing and emerging governance frameworks. The analyses of these frameworks is not exhaustive, but they are designed to highlight the critical features of the governance landscape. Once this is complete, the focus shifts to the challenges in each area of activity, followed by an analysis of the potential for standards-based solutions.

3.1. Data collection and use

Some of the most contested questions in discussions of data governance concern how data should be collected and used. While Canada's data governance framework is in need of an update (Scassa 2019), other jurisdictions such as the EU and California have developed innovative new legislative and regulatory frameworks. These and other frameworks offer a variety of potential approaches for responding in an innovative manner to the challenges posed by the increasingly ubiquitous collection and use of data.

3.1.1. Current governance landscape

In Canada, data collection and usage is governed by a small constellation of federal and provincial laws. Federally, the most important of these are the *Privacy Act,* which governs the personal information-handling practices of the federal government, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which regulates how private firms and not-for-profit organizations must handle personal information (Privacy Commissioner of Canada, 31 January and 9 January, 2018). Provincially, different governments have passed a series of similar laws to govern areas of provincial responsibility (Privacy Commissioner of Canada, 31 January, 2018). For instance, the Province of Ontario has passed the Freedom of Information and Protection of Privacy Act (FIPPA), the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and Personal Health Information Protection Act* (PHIPA).

While not without differences, the overarching purpose of these laws is to ensure that individuals' personal information is adequately protected whenever it is collected and used and wherever it is held (Privacy Commissioner of Ontario, July 2014a, July 2014b, and August 2014; Privacy Commissioner of Canada, 31 January and 9 January, 2018). Generally, the collection and use of personal data requires informed consent on the part of the data subject. If the data holder wishes to use it for a purpose beyond that for which it was originally collected, data holders are generally required to seek consent from the data subject. Some of these laws provide citizens with processes for accessing their data, challenging its accuracy and correcting it. Generally, they also create a privacy commissioner or a similar officer responsible for overseeing the privacy regimes that the laws create.

Increasingly, however, these laws are in need of updates. For example, and as is discussed below, the "notice and informed consent" model on which they are based is widely seen as broken. Specifically, data collectors often seek to maximize their freedom in how they use the data they collect without needing additional consent by making the Terms of Service (ToS) agreements by which they obtain individuals' consent long, extremely broad, difficult to understand and subject to change without notice. Consequently, most users accept these agreements without ever reading them. They give consent, but it is not "informed" (Stinson, 2018).

In response, some jurisdictions have enacted new rules aimed at addressing these and other concerns. The EU's *General Data Protection Regulation* (GDPR) is the most important of these, and its main data-related features include:

- Strengthened consent requirements for firms that collect and use user data.
- A requirement for data holders to notify users if their data has been breached.
- A right for users to obtain electronic copies of any personal data held by the organization free of charge.
- A right to be forgotten.
- A data portability requirement.
- Integration of the "privacy by design" concept.
- A requirement that many data holders appoint a Data Protection Officer (EU GDPR.org).

While the GDPR is a European instrument, its jurisdiction extends beyond the EU to any organizations that collect data from EU residents. Because of the size and importance of the EU market, many non-EU firms have decided to comply with GDPR worldwide to avoid errors or use its provisions as a global best practice. Other jurisdictions are already building on the GDPR's advances. For instance, California recently passed a law, set to come into effect in 2020, that prohibits firms from denying users service if users decline to have their data collected beyond what is absolutely necessary for the functioning of the service (Lapowsky, 2018).

The GDPR is a new law and many of the details of its interpretation and enforcement are still to be determined. In this context, a number of standards are beginning to play important roles as instruments that organizations can use to demonstrate good faith efforts at compliance. Some examples include:

- *ISO/IEC 19944:2017 Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use*
- *ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification techniques*
- *ISO/IEC DIS 27552 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*
- ISO/IEC *38505-1:2017 Information technology – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data (Girard 2019, p. 16)*

More such standards are in development, such as *ISO/NP 31700 Consumer protection – Privacy by design for consumer goods and services.*[2]

In addition to GDPR compliance, there are also some important data-related standards being developed by the ISO/IEC JTC 1/SC 42 committee. This committee, which is focused on developing AI standards, is working on a number of data-related standards because of the importance of the high quality data for training AIs. These include *ISO/IEC TR 20547-2:2018 Information technology – Big data reference architecture – Part 2: Use cases and derived requirements and ISO/IEC TR 20547-5:2018 Information technology – Big data reference architecture – Part 5: Standards roadmap*, as well as three other standards in development, which are all focused on Big Data reference architecture.[3]

In Canada, the CIO's Strategy Council is developing a standard on data access and privacy *(CIOSC 100).*[4] The Government of Canada has developed its own internal "standards" called the Government of Canada Digital Standards. These "standards" are quite high level and serve more as a set of guidelines than a set of standards as traditionally understood, but they could serve as a foundation for future standards.[5]

Other instruments are emerging to play standards-like roles as well. Powerful firms, for instance, are already acting as *de facto* regulators in some areas. Apple's recent move to block an app called "Facebook Research" from running on its mobile operating system is one example (Feldman, 2019). The app enabled Facebook to track everything a user was doing on their phone (Constine, 2019). Apple claims the app violated their ToS or, viewed another way, did not meet the data "standards" Apple uses to govern its platform.[6]

3.1.2. Challenges

The importance of data is growing exponentially. In terms of simple quantity, around 90 per cent of all the data that has ever been created by humanity was created in the past two years (Marr, 2018). This growth brings with it enormous challenges; below we highlight two of the most important from a Canadian perspective.

The "notice and informed consent" regime

The first challenge that needs to be addressed concerns Canada's "notice and informed consent" regime. Concern about widespread online data collection is expanding into new spaces like homes, cars and public spaces thanks to data-hungry technologies like voice-operated virtual assistants, self-driving cars (Seals, 2018) and smart cities (Rizza, 2018). Although Canada's existing privacy regime requires that collection of personal data be limited to the minimum required for fulfilling the stated purposes of a service, technology companies are nevertheless using broadly worded ToS agreements to stockpile highly detailed user profiles and use this data for secondary uses.

[2] See https://www.iso.org/committee/6935430.html

[3] See https://www.iso.org/committee/6794475/x/catalogue/p/1/u/0/w/0/d/0 and https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0

[4] See https://ciostrategycouncil.com/standards/new-projects/

[5] See https://www.canada.ca/en/government/publicservice/modernizing/government-canada-digital-standards.html

[6] There are many other examples of Apple and Google denying access to their app stores to developers. See, for example, the story of the Disconnect app (Ezrachi and Stucke 2016, p. 178-190).

"The importance of data is growing exponentially. In terms of simple quantity, around 90 per cent of all the data that has ever been created by humanity was created in the past two years."

Rebuilding a more effective consent model is critical, both from a moral perspective – the "surveillance capitalism" business model that has emerged is being blamed for many negative side effects including rising mental health problems and increasingly polarized politics (The Economist, October 2018) – and also, a legal necessity. Specifically, PIPEDA was originally passed because Canada's data protection laws did not meet the standards required to allow data transfers from the EU to Canada (Scassa 2018, p. 7). The fact that Canada's data protection laws have again fallen behind Europe's means that Canada may once again be forced to update its data protection regime or risk losing data interoperability with a market of over 512 million people.

The need for industrial data standards

While updating the current consent regime for personal data is critical, it is important that doing so does not block efforts at addressing Canada's second important data collection challenge. While there is arguably too much collection of personal data, there is actually far too little industrial data collection and sharing in Canada. The creation of industrial standards will be critical to unleashing Big Data's full potential for Canada's economy.[7]

Access to data, particularly non-personal industrial and commercial data, will be essential to future economic success, both for individual firms and nationally. The ability to collect this data – in the right format, and at a high level of quality – will be critical to the optimization of industrial and commercial processes, the design of new products and services, and the creation of valuable new tools like AIs. This will also be true for the establishment of the data value chains and markets on which this optimization will depend.

According to one expert interviewed for this report, the growth of some Canadian firms may already be slowing due to data shortfalls. This view is not universally held, but this expert suggested that this may be occurring because access to private venture capital for AI companies may be decreasing in Canada because these venture capitalists see Canadian AI companies as not having access to enough data to create and sell their products and scale up. While data-sharing, swapping, licensing or buying and selling data could be mutually beneficial for firms, few are currently willing to do so. This reticence is partially due to privacy concerns, indicating problems with the privacy regime and a lack of clarity regarding acceptable data de-identification, anonymization and aggregation techniques and practices (Hirsh, 2019).

Organizations are also unwilling to exchange data because they are unsure if the data in question is of sufficient quality. Organizations are concerned that this could result in contaminated data pools being used to train a biased AI that would make mistakes for which

[7] This point was made by multiple experts interviewed for this project.

they could be held liable. In other words, because the data governance regime, including data quality standards, remains underdeveloped, uncertainty is blocking economic development. Overcoming this challenge and finding a way to enable a broader and more liquid data market will be critical. Otherwise, it will be extremely difficult for firms other than those that are already rich in data to benefit from AI, which may hurt Canada's competitiveness.

3.1.3. Analysis and Opportunities

Overcoming these challenges will require action on multiple fronts, including action by governments and regulators, policy changes and international collaboration. Significantly, there are good opportunities for standards-based solutions to make a positive contribution to these efforts.

"Safe harbours"

The most obvious opportunity involves building on top of existing standards that are already proving valuable. As mentioned earlier, organizations seeking to comply with the GDPR are already using adherence to certain standards to demonstrate good faith efforts at compliance. Thus, opportunities exist to develop new standards, or modify existing ones, in ways that provide "safe harbours" for many of the GDPR's requirements and those associated with California's *Consumer Privacy Act* (Roettgers, 2018).

While a more in-depth examination of GDPR than is possible here would be required to provide an exhaustive list of specific opportunities, one example stands out. Currently, there is still significant uncertainty around best practices for the Data Protection Officers that the GDPR requires organizations to appoint (Joyce et al.). Thus, the development of a management standard (similar to the ISO/9001 or the ISO/IEC 27000 families of standards) that helped to codify best practices based on consensus expert opinion could be useful.

Enabling data-based value chains and markets

Standards and SDOs have an opportunity to play a role in laying the foundations for viable data-based value chains and markets. For example, one report has identified the following four opportunities:

1. Standardization depends on a shared vocabulary encompassing an ontology, taxonomy, semantics, definitions and terminology. Developing a shared vocabulary for data is a critical first step towards enabling interoperability.
2. The development of standards for the structuring and categorizing of shared information environments and datasets is another opportunity. This would include standards for organizing and labelling categories of datasets capable of supporting "usability, retrievability, explorability and traceability" (Girard 2019, p. 14).
3. Enabling bulk sharing and selling of data will require a classification system that can support reliable, and perhaps automated, differentiation between forms and qualities of data.
4. In more sensitive cases, such as with personal identifiable information, a standards-based approach could provide an additional taxonomy that would enable reliable coding of data on additional characteristics, including:
    a. source (e.g. social media or government database)
    b. sharing permissions (e.g. consent has been granted for usage by the collector, by a specific third party, only on a non-exclusive basis)
    c. permitted usages (e.g. original use only, original use plus some specific additional uses)
    d. de-identification status/level
    e. aggregation status/level (Girard 2019, p. 14-16)

Addressing the concern raised earlier regarding liability for the corruption of datasets will likely require new legislation to properly balance the costs and benefits of using Big Data (The Economist, 8 April, 2017a). Nonetheless, the development of standards along the lines outlined here could help reduce liability concerns, as well as the search, evaluation and transaction costs involved in identifying useful data. In so doing, standardization would help to "commodify" data while also protecting privacy. This would enable the establishment of the data-based value chains and broader and more liquid data markets needed to unlock the full benefits offered by Big Data and AI.

Consumer-facing standards

The steps described above apply primarily to the business-to-business aspects of data collection and use. There are also opportunities to create consumer-facing standards that could enable organizations to indicate their adherence to instruments like the GDPR.[8] Such a system could be useful for differentiating between products and services that comply with instruments like the GDPR and those that do not. Additionally, the creation of such standards could also generate opportunities for certification, an area where demand is likely to increase and SDOs will be well-placed to respond.[9]

One of the obstacles to consumer-facing standards, however, is the question of how to reliably identify organizations, products and services that have received a specific certification. Graphical labels of attestation or kitemarks which an organization can display are not particularly useful because they can be easily copied and forged in a digital context. Similarly, the use of registries, which accreditation bodies already use to list products that have been certified against a particular standard, do not represent a robust solution. These registries are not well-known by consumers and, even if they were, checking them adds steps to the shopping process, something that significantly reduces their use by consumers.

Finding a way to remove these extra steps by reliably automating verification might be the difference between success and failure.[10] The advent of blockchain and distributed ledger technology may offer a potential solution to these problems. In such a system, certifications could be tokenized and hosted on a ledger maintained collaboratively by a group of accredited certifying organizations. The use of a distributed ledger would ensure reliability while the linking of many accrediting organizations would help raise the system's profile and improve its convenience.

A digital ledger could provide the foundation for a system in which web browsers could automate the process of evaluating a website or app's accreditation by automatically inspecting the distributed ledger. This could enable the development of web browsers into which users enter their privacy preferences as default settings and set the browsers to warn them when a website's accreditations do not meet these preferences.[11] Researchers have already developed some tools, like an AI and an associated chatbot called Polisis and Pribot, which will read and interpret websites and apps' ToS agreements, which offer an early indication of how such a system might work (Greenberg, 2018). But by combining a digital ledger with "machine readable standards," – that is, standards to which adherence can either be established by an algorithm or reliably indicated digitally – the approach described here could make this system even more reliable and efficient.

Standards for a decentralized web

There are currently a number of projects underway designed to enable users to take greater control over their own data. One example is the Solid project being led by Sir Tim Berners-Lee, inventor of the World Wide Web.[12] This project is designed to enable users to maintain their own data stores and control the extent to which websites, apps and other users are able to access it. For example, instead of sharing photos with friends by uploading these photos to Facebook – which then has a licence to use the photos as they wish – users would upload the photos to their own personal online data stores (or PODS) and share access with their friends or firms through "dApps" or decentralized apps. Unlike existing apps like Facebook, however, these dApps would not store user data. Rather, they would simply provide a user interface and facilitate the linking of individuals' data.

[8] The Sharing Economy TrustSeal is one limited example of an attempt to create a management standard for largely digital organizations. Its focus is on much more than data. See https://sharingeconomytrustseal.com/

[9] A number of experts interviewed for this report made this point.

[10] This point was suggested by a standards expert interviewed for this report.

[11] While such a system will naturally be constrained by users' digital literacy, the question of how to increase users' digital literacy so that they can take advantage of any new tools offered to them is beyond the scope of this report.

[12] See https://solid.inrupt.com/

"If current security practices are not improved, much of this data will only be protected minimally, if at all."

Standards will be even more essential in such a decentralized context than in the current one where firms like Google and Facebook hold and manage user data according to their own internal standards. Indeed, without standards, the interoperability and compatibility required by this decentralized system will not be possible.

3.2. Data security

Data security is the second area of data governance covered in this report. Data security is critically important because of how it undergirds data collection and usage. It makes no sense to exert significant effort collecting and using data properly while leaving this same data vulnerable to theft or corruption by hackers or spies. With more data being stored than ever before, and with a seemingly endless parade of data breaches at firms like Starwood-Marriott (Valinsky, 2018), Equifax (Ng, 2018) and Yahoo (Larson, 2017), the importance of security is clear for both citizens and policymakers.

Moreover, the importance of data security will only grow as the expansion of the IoT gathers speed. In 2006, it was estimated that there were only 2 billion devices connected to the Internet. By 2015, that number, which had by then begun to include large numbers of IoT devices, had reached about 15 billion. Projections suggest that this number will reach 200 billion in 2020 (A Guide to the Internet of Things). Already, fridges, smart speakers, thermostats, toys and a host of other household items are routinely connecting to the Internet. These devices will soon be joined by smart roads, clothes and many other everyday items. All of these devices will be collecting, storing and transmitting previously unimaginable quantities of data. Unfortunately, if current security practices are not improved, much of this data will only be protected minimally, if at all (BBC News, 2017).

3.2.1. Current governance landscape

As is the case with data collection and usage, the starting point for data security in Canada lies in the constellation of privacy laws enacted by the federal and provincial governments. The key security themes in these laws are that data should only be stored if it is needed to fulfill the purpose for which it was collected and that organizations should employ the appropriate safeguards needed to secure that data.[13] Additionally, just as with data collection and usage, and for essentially the same reasons, the GDPR plays an important role in governing data security in Canada as well.

Some voluntary data security standards also exist such as the *ISO/IEC 27000* family of standards focused on information security management systems. Unfortunately, because organizations are either unaware of these standards, do not prioritize security, or their partners do not require it of them, organizations often fail to

[13] For instance, see this summary of CSA Group's model code, on which PIPEDA was based: https://www.cippguide.org/2010/06/29/csa-model-code/

implement these standards. This is indicative of a wider failure to take data security seriously which is discussed further below.

Given that many of the organizations that collect Canadians' data are based in other countries, especially the USA, it also important to note the main US data security instruments. Unfortunately, the situation in the USA is quite similar to Canada in that data security is not particularly robust, though some of the large technology firms, such as Google, Apple and Microsoft are recognized as having strong internal data security practices (Schneier 2018, p. 20). Nonetheless, existing US standards may be applicable in Canada or could serve as inspiration for Canadian standards.

The most important US data security standard is the National Institute of Standards and Technology (NIST) set of cybersecurity standards called the *Framework for Improving Critical Infrastructure Cybersecurity*. This framework is a "comprehensive guide for private-sector organizations to proactively assess and minimize their cybersecurity risk" (Schneier 2018, p. 123). The standard is voluntary but, since 2017, compliance has been mandatory for federal agencies (Schneier 2018, p. 123). The US government has a similar security assessment and authorization process for cloud services used by federal agencies called the *Federal Risk and Authorization Management Program* (FedRAMP) which also involves compliance with a number of NIST cybersecurity standards.[14] Given that these standards are voluntary outside of government, implementation in the private sector is limited.

3.2.2. Challenges

The greatest challenge in data security is that data holding organizations, especially private-sector firms, do not take security sufficiently seriously. Even though security standards exist, few firms bother or are able to employ them.[15] For example, following the massive Equifax data breach in 2017, a US House of Representatives Oversight Committee found "that Equifax's security practices and policies were sub-par and its systems were old and out-of-date, and bothering with basic security measures — like patching vulnerable systems — could've prevented its massive data breach last year" (Whittaker, 2018). In other words, approximately 155 million people had their personal data breached because Equifax failed to fix a vulnerability in their software for which a patch had been made available two months earlier (Schneier 2018, p. 37).

Attenuated value chains for data collecting devices

Why is data security so poor? For many firms, ensuring data security is very difficult because the value chains for electronic devices that collect and transmit data are becoming increasingly long and complicated. These value chains also often involve many different firms and (often temporarily assembled) engineering teams, spread across multiple countries, all of which have very tenuous connections with each other (The Economist, 8 April, 2017b). As all of these individuals and organizations are only responsible for small parts of the larger security whole, there is little incentive or opportunity for any of them to take on the onerous responsibility of figuring out how to coordinate security across the entire chain.

Limited liability

This division of responsibility would not be a problem if responsibility for breaches in data security was clearly assigned and resulted in meaningful consequences. Surprisingly, however, software firms are generally not held liable for flaws in their software even if these flaws are responsible for data breaches. Without consequences for these breaches, firms do not have sufficient motivation to take on the difficult task of instilling security discipline into their long and complicated value chains. This lack of motivation is further entrenched by the failure of the market to reward organizations that compete on the basis of robust privacy or data security features.

3.2.3. Analysis and Opportunities

A key challenge for data security lies with how many devices used for collecting and transmitting data are insecure. This problem will get worse before it gets better as the number of Internet-connected devices in the IoT continues to expand rapidly. This expansion

[14] See https://www.fedramp.gov/nist-publications/

[15] This point was emphasized by a cybersecurity expert interviewed for this report.

will also necessarily result in much greater pressure to improve the rudimentary systems for building data security into these devices. This pressure presents a host of opportunities for standards and SDOs.

Increased motivations for improved security

As computers and Internet connections are integrated into more and more devices, the possibility for security breaches to cause significant harm is rising. Hackers have already shown that they can remotely hijack a car using its onboard computer systems (Greenberg, 2015). Critical infrastructure such as electric power systems have recently come under attack with real physical damage occurring and the clear possibility for loss of life (Vallance, 2016). As the real costs in human life and suffering mount, governments will be forced to take action to ensure network and data security (The Economist, 8 April, 2017a).

Similarly, as Internet-enabled devices expand into new areas, the existing immunity of software developers to liability will become untenable. While it might have been acceptable for an operating system to crash if the only result was that office workers lost a few hours of their work, it will not be acceptable for an autonomous vehicle's operating system to crash if the result is a multiple fatality collision.

In many ways, the current state of cybersecurity is analogous to the situation in the petrochemical sector 100 years ago and the electrical sector 75 years ago.[16] As these young industries developed and their value chains became longer and more complex, their products became less safe and accidents proliferated. In both cases, a professional class critical to the sectors' success, namely engineers, identified a professional obligation to solve these problems. They did so by self-organizing and by introducing standardization into the value chains to ensure the quality of components and inputs. While a professional class of developers and software engineers is still at an incipient stage, these professions are taking steps towards implementing the educational and institutional frameworks needed to ensure safety and security of their products and services. Nevertheless, progress to date has been limited (CBC Radio, 2018).

Security by design

Just as the inclusion of the concept of "privacy by design" in the GDPR represented an important step towards greater privacy, "security by design" will be critical to improving data security. While governments may be able to identify such a concept as the objective of a larger cybersecurity governance regime, they are unlikely to be able to develop a comprehensive program for its realization over time.

This represents an opportunity for SDOs which are well-placed to convene relevant experts and stakeholders to help develop a set of principles that would define this concept and provide a foundation for a data "security by design" standard. These principles may include:

1. Minimize data collection.
2. Store and transfer data securely.
3. Minimize data use.
4. Be transparent in data collection, use, storage and deletion.
5. Anonymize data wherever possible (i.e. anonymize by default).
6. Allow users to access inspect, correct and delete their data.
7. Delete data when it is no longer needed (Schneier 2018, p. 109-110).

Many of these principles are already a part of the GDPR. As discussed in the context of data collection and use, standards are playing a role in operationalizing these principles by providing instruments that organizations can use to demonstrate good faith efforts at adherence. This same opportunity exists for data security, and standards like *ISO/IEC 27000* and the NIST standards described earlier could potentially play this role.

[16] A cybersecurity expert interviewed for this report made this comparison.

"Just as the inclusion of the concept of "privacy by design" in the GDPR represented an important step towards greater privacy, "security by design" will be critical to improving data security."

Data security is cybersecurity

Due to the way data security is intertwined with broader cybersecurity, focusing narrowly on data likely understates the opportunities for standards to play a role in data security. The following ten principles for IoT security, assembled from a wide range of organizations and governments, could serve as an important program for advancing cybersecurity more generally (Schneier, 2017).

1. **Be transparent**, especially in describing how a device's security system works, the threats it counters, the ones it does not and the length of time the device will be supported.
2. Make devices' software **reliably patchable**, patch vulnerabilities quickly when they are discovered, and ensure that devices update their software regularly.
3. All software should be **tested in pre-production** before it is released.
4. Devices should be **secure out of the box** so that it is not up to users to configure them. This means no weak or default passwords, ubiquitous use of two-factor authentication and the disabling of remote administration features if possible.
5. If a device is not able to connect to the Internet, it should **fail predictably and safely**.
6. **Standard protocols** are generally more secure and better tested than custom built ones and should be used whenever possible.
7. Products that contain **known vulnerabilities should not be put on the market**.
8. An **IoT device's core functionality should still operate** even if all network connections have been severed.
9. Data on a device should be **encrypted in storage and transmissions** to and from the device should be encrypted and authenticated.
10. Organizations should **allow security research on their products**, welcome vulnerability reports, and avoid hostility to researchers (Schneier 2018, p. 108-109).

By identifying standards that help to operationalize these principles, and by developing new standards where necessary, SDOs could make a significant contribution to addressing the threat to data security that lurks in poor overall cybersecurity.

Enabling insurance

These lists represent important potential starting points. But even if the content of a data security standards framework is available, many of the problems in data security stem from a lack of motivation to increase security, not from a lack of ideas for how to do it. This is likely to change in the near future as public pressure and increased liability make it harder for software firms and device makers to continue treating security as a low priority.

One of the ways that this problem may be solved is through the creation of a robust and sophisticated cybersecurity insurance market (The Economist, 23 August, 2018) – something that SDOs are well-positioned to facilitate. Currently, the market for cybersecurity insurance is fairly underdeveloped. Nonetheless, as exposure to liability grows, organizations will seek to insure themselves and insurers will seek ways to measure the risk levels associated with writing policies for these clients. SDOs could provide a helpful service by working with insurers to make them more aware of existing cybersecurity standards and developing new cybersecurity standards.

These standards could form the basis for certification programs. Insurers could use these certifications by linking premiums to the level of accreditation held by the organization being insured. Government could encourage this process by requiring that certain types of IoT-enabled devices be insured as a condition of their sale (The Economist, 8 April, 2017a). Increased liability for software flaws and for poor data security practices, already starting to appear through class action lawsuits,[17] combined with rising software insurance costs, would provide strong economic incentives for firms to implement these standards (The Economist, 8 April, 2017b).

The changing role of traditional SDOs

Despite these many opportunities, the fact that traditional standards development processes are viewed as too slow by many who work in data security remains an obstacle to standards playing a larger role in data security. Given the number of existing standards that have already been identified in this section, there is clearly a role for traditional SDOs in this sector. Nonetheless, there are also some opportunities for SDOs to evolve in ways that would make them a better fit for this increasingly fluid governance context.

One potential opportunity for SDOs to enhance their role in the digital economy would be for them to focus less on the development of standards, and more on becoming trusted certifiers of open standards developed by others, especially the open source community.[18] This might be especially important in data security if cybersecurity insurance develops as described earlier. Another potential opportunity would be for accredited SDOs to update their processes so that they became quicker, possibly by adopting or adapting practices from unaccredited organizations like the Internet Engineering Task Force (IETF).[19]

Additionally, just as standards represent a faster and more flexible complement to laws and regulations, the emergence of open source standards and protocols may represent a qualitatively new form of rule instrument best integrated into the traditional standards landscape as a faster and more flexible complement to traditional standards. In this model, traditional SDOs could continue to focus on higher level principles, management practices and assembling wide arrays of stakeholders to ensure that all relevant perspectives are integrated. These higher level principles-focused instruments would then include ambulatory references to the more specific open standards in a manner analogous to how legislation and regulations use ambulatory references to traditional standards.[20]

Digitizing standards

Finally, there may be opportunities to improve data security by bringing standards themselves more fully into the digital age. For example, a central problem identified earlier is that the market has failed to produce competition between firms on the basis of data security. The development of standards for data security would be an important first step to enabling this sort of competition, but would be unlikely to be enough on its own as the public is not sufficiently educated on data security.

[17] For example, see Fraser (2018) or, for small claims actions, Murphy Jr (2018).

[18] This idea was provided by an open source expert interviewed for this project.

[19] This idea was proposed by an open source expert interviewed for this report. See https://www.ietf.org/standards/process/informal/ Accredited SDOs are SDOs that have been accredited by national standards bodies (NSBs) which are in turn bodies that have been designated by national governments as the official accreditors of SDOs in that country.

[20] See Ditta et al. 2017, 41. An ambulatory reference to a standard is a reference to a standard in regulation or legislation that references a standard but not a specific version of the standard. The understanding is that when the version is not stated, the reference is automatically interpreted as being to the most recent version of the standard. Thus, ambulatory references have the virtue of enabling governments or regulators to reference a standard and not need to update their rules, processes which can take significant time and effort and which are often neglected, every time a new edition of the standard is developed.

By making it easier to evaluate a digital product or service's security characteristics, the establishment of a consumer-facing system of machine readable standards and a digital compliance registry compatible with web browser plug-ins, as discussed in the preceding section, might enable much more robust security competition. Not only could such an approach improve the consumer marketplace, it could also improve the business-to-business marketplace given that small and medium-sized enterprises are in similar positions to the average consumer when it comes to evaluating their data security needs.

4 Algorithms and AI

The word algorithm has recently acquired an opaque shroud of connotations which threaten to obscure its true meaning. In reality, the term algorithm simply refers to a process that has been established for the achievement of a particular goal. Algorithms are often compared to recipes, that is, a set of instructions detailing how to produce a particular outcome (Brogan, 2016).

One of the reasons that algorithms have drawn such interest is because of their association with AI. AI is a general term which refers to a class of complex algorithms written in computer code. Increased use of algorithms, especially AI algorithms, offers significant benefits, but also carries significant challenges. Indeed, because of how AI is inextricably linked to the data on which it is trained, many of the same issues which were raised in the preceding section cascade into the consideration of algorithms as well.

Moreover, the growing ability of AIs to reach decisions which transcend human comprehension raises novel questions. Some of these questions are explored below through an examination of the opportunities that exist for standards to play a role in two specific aspects of algorithmic governance: helping humans make better decisions and on the use of algorithms to set prices dynamically.

4.1. Algorithmic decision-making

Algorithmic decision-making can potentially offer many benefits. For example, the Conference Board of Canada estimates that the introduction of autonomous vehicles, which would be controlled by algorithms, could eventually reduce the annual number of road accident fatalities in Canada from about 2,000 to around 400. They also suggest that the introduction of autonomous vehicles could result in an overall economic benefit to Canada of over $65 billion a year (McDonald, 2018).

The spread of algorithmic decision-making is also raising concerns about the ability of algorithms to adequately incorporate ethics into their decision-making as well as a variety of other potential impacts. Consequently, there has recently been an explosion of proposals for rule instruments designed to ensure that society is able to access the benefits of algorithmic decision-making while avoiding its pitfalls.

4.1.1. Current governance landscape

Given the close connection between algorithms and data, many of the rule instruments identified earlier in the data governance section either apply directly or indirectly to algorithms. The GDPR also contains an article (22) focused specifically on algorithmic decision-making. It states that individuals "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" [Regulation (EU) 2016/679].

While this prohibition suggests that the GDPR will limit the use of algorithms in making decisions that impact EU residents, it is qualified in a number of ways elsewhere in the GDPR (Wachter et al., 2017). For example, the EU and its member states are able to make laws which allow "automated decision making" so long as they explain how these processes can take "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" [Regulation (EU) 2016/679]. Consequently, the full extent of the GDPR's prohibition will only become clear through judicial interpretation.

Box A

1. **Transparency:** the rules by which an AI takes decisions should be made available.
2. **Human control:** Final decisions should either rest in the hands of a human or should be appealable to a human decision-maker.
3. **Notice:** Humans should be informed when they are subject to an AI decision-maker.
4. **Non-discrimination:** AI should not be unfairly biased against particular groups.
5. **Responsibility:** The entity using an AI should retain responsibility for its decision.
6. **Data quality:** Users and developers of AI should know the provenance of the data used to train it and ensure that only correctly obtained data and data consistent with principles like non-discrimination is used.
7. **Intelligibility:** The reasons for a decision must be made available to those impacted by them and must not be unreasonably obscured by complexity.
8. **Oversight:** Uses of AI systems must be subjected to democratic scrutiny, debate and control.
9. **Prudence:** Development and deployment of AI should proceed cautiously with those involved anticipating, as far as possible, potential adverse impacts and mitigation strategies.
10. **Sustainability:** AI should be developed and operated in an environmentally sustainable way.
11. **Shared Benefit:** The development of AI should benefit as many people as possible.

While there are not many other laws or regulations which specifically govern the use of algorithms,[21] the past few years have seen the development of a large number of declarations aimed at establishing conceptual frameworks for the governance of AI in particular.[22] While there is substantive diversity in these declarations, a number of core principles are shared across multiple declarations (see Box A).

Several governments have also developed policies for the use of AI systems.[23] In Canada, the federal government has developed a set of guiding principles for the responsible use of AI[24] and a Directive on Automated Decision-Making which will come into full force in 2020.[25]

Internationally, the ISO/IEC JTC 1/SC 42 committee is a central site of standards development for AI. This committee has already published two standards on Big Data reference architecture, a critical prerequisite for making data available and usable for the training of machine learning algorithms. The committee also has ten other standards under development in areas ranging from additional work on Big Data, to concepts and terminology, to bias in AI systems.[27]

Another important site of AI standards development is the Institute of Electrical and Electronic Engineers (IEEE) Global Initiative on Ethics of Autonomous and Intelligent Systems. This initiative's objective is to ensure stakeholders involved in the development of AI systems are "educated, trained, and empowered to prioritize ethical considerations so that these technologies are advanced for the benefit of humanity." The initiative is also advising the IEEE as it formulates the IEEE P7000 family of standards for AI. There are currently 11 working groups focused on producing standards in areas ranging from processes for addressing ethical concerns during AI system design to wellbeing metrics standards for AI systems.[28] Finally, in Canada, the CIO Strategy Council is also developing a standard focused on the ethical design and use of AI systems *(CIOSC 101:2018).*[29]

[21] Malta's law governing the possible implementation of an autonomous corporation is one very interesting exception (Ronstedt and Eggert, 2018).

[22] See, for example, The Toronto Declaration https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/, the Universal Guidelines for Artificial Intelligence https://thepublicvoice.org/ai-universal-guidelines/, The Montreal Declaration for a responsible development of artificial intelligence https://www.montrealdeclaration-responsibleai.com/the-declaration, UNI Global Union 10 principles for AI http://www.thefutureworldofwork.org/opinions/10-principles-for-ethical-ai/, and the Asilomar AI Principles https://futureoflife.org/ai-principles/?cn-reloaded=1 to name just a few.

[23] See https://www.nesta.org.uk/data-visualisation-and-interactive/mapping-ai-governance/ for a comprehensive list.

[24] See https://www.canada.ca/en/government/system/digital-government/responsible-use-ai.html

[25] See http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

[26] See https://www.iso.org/committee/6794475/x/catalogue/p/1/u/0/w/0/d/0

[27] See https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0

[28] See https://ethicsinaction.ieee.org/

[29] See https://ciostrategycouncil.com/standards/new-projects/

"Because of how AI draws on historical data, it is prone to reproducing biases encoded in this data."

4.1.2. Challenges

Building the governance instruments required for the successful governance of algorithmic decision-making will require stakeholders from across a host of sectors, institutions and parts of society to come together to overcome a variety of different challenges.

Bias

Because of how AI draws on historical data, it is prone to reproducing biases encoded in this data. One of the first instances of this problem that has come to light involves an algorithm that was used in Florida to predict how likely a prisoner was to commit a future offence. The "risk score" that the algorithm generated was used by judges to help them decide whether to grant bail, how large a bond to set, and how to structure convicts' sentences and parole requirements (Angwin et al., 2016). Drawing on prevalent systemic racism, this algorithm incorrectly labelled black prisoners as future criminals at almost twice the rate that it did white prisoners and labelled white prisoners as low risk more often than black prisoners (Angwin et al., 2016).

Algorithmic decision-making has also been used in "predictive policing," an approach in which algorithms predict the areas of a city in which crimes are more likely to be committed (Rieland, 2018). These systems have been criticized as biased because they can be prone to feedback loops. These loops arise because areas, such as low income or ethnic minority neighbourhoods, have been policed disproportionately in the past. Consequently, these areas make up a disproportionate percentage of a city's discovered crime – a key input into the algorithm (Rieland, 2018). These areas are labelled by the algorithm as priority areas, leading to an even more disproportionate police presence. Unsurprisingly, this disproportionate presence then tends to result in the discovery of even more crime, such that these neighbourhoods then account for an even larger percentage of a city's discovered crime, regardless of the true crime rate. This results in even more policing resources being assigned to the neighbourhood and the feedback loop continuing (Ensign et al., 2018).

Inclusion

Another way in which individuals can be disadvantaged by algorithmic bias involves individuals who find themselves on the edges of a "normal distribution." The normal distribution, also called the bell curve, is a mathematical term that refers to the tendency, observed when many phenomena are represented graphically, for data points to cluster around a central core with a much smaller number of points scattered around the outskirts. (See Figure 3).

***Figure 3 –** Typical Scatterplot of a Normal Distribution*

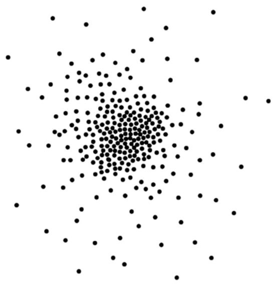
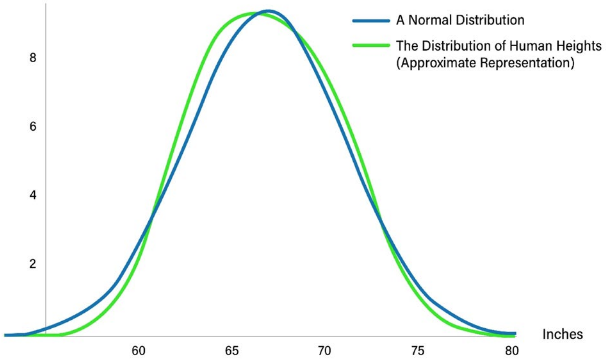


Image inspired by Treviranus (2018). Original image subject to an Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Creative Commons Licence https://creativecommons.org/licenses/by-nc/4.0/

A classic example of this tendency is the approximately normal distribution of adult human height (See Figure 4).

Figure 4 – *Approximate Distribution of Human Height Compared to a Normal Distribution*



Note: The graphic is illustrative and not exactly representative of actual data.

Normal distributions are important for algorithmic decision-making because algorithms usually make decisions on a probabilistic basis. That is, their decisions are based on what the data on which they have been trained suggests is most likely to occur. The problem that arises when the training data is normally distributed is that those individuals who fall outside the core where most humans tend to cluster, are often marginalized by the algorithm that always makes decisions on the basis of that core. (See Figure 5).

Figure 5 – *How Probabilistic Decision-making Marginalizes Outliers*

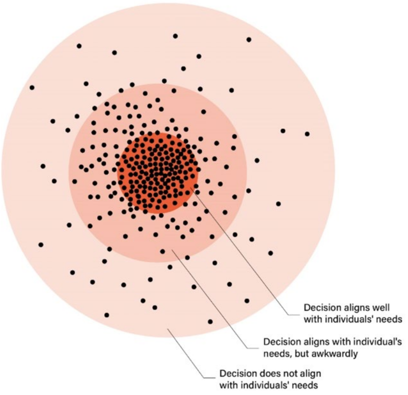

Decision aligns well with individuals' needs
Decision aligns with individual's needs, but awkwardly
Decision does not align with individuals' needs

Image inspired by Treviranus (2018). Original image subject to an Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Creative Commons Licence https://creativecommons.org/licenses/by-nc/4.0/

For instance, researchers have documented how individuals with anomalous characteristics can present unsolvable riddles for algorithms trained on data representative of the larger population. For example, in one simulation, an algorithm designed to direct autonomous vehicles was presented with a scenario in which an unorthodox wheelchair user, who propels herself with her legs backwards, was crossing a road. In this case, the algorithm predicted the person's direction of travel incorrectly and ran them over (in the simulation). In an effort to correct this error, the algorithm was fed additional training data and the simulation was run again. Researchers noted an important change in the behaviour of the hypothetical autonomous vehicle: the second time around, it ran the wheelchair user over with even greater confidence (Treviranus 2018).

This problem, which is representative of a larger class of problems, derives from the fact that because algorithms are guided in their decision-making by probabilities, their decision-making is essentially determined by the characteristics of those who can be found at the centre of the normal distribution, a "homogeneous mass that privileges the mean" (Treviranus 2018). Anomalous individuals who find themselves on the fringes are either removed from consideration to make decision-making clearer for the algorithm, or are probabilistically overwhelmed by the mass at the centre (Treviranus 2018). Thus, in cases where an anomalous individual finds themselves alone on the fringe, further training the algorithm with additional pools of data representative of the larger population can actually make the situation worse as it is likely to only reinforce their anomalous position and thus, the algorithm's lack of focus on them.

Transparency and accountability

A big problem with bias in algorithmic decision-making is that it can be difficult to spot. As discussed earlier, this bias is often the result of the data on which the algorithm was trained being tainted by pre-existing societal biases. Because these biases often align with pre-existing societal ones, they can be harder to recognize.

Additionally, it is usually impossible to spot a bias on the basis of a single decision rendered by an algorithm. The only way to substantiate a claim of bias is to review a representative sample of decisions and analyze this larger pool to see if there is evidence of algorithmic bias. Acquiring the information needed to do so could be difficult, especially if the organization using the algorithm would prefer not to attract criticism.

Ideally, it would be possible to inspect the algorithm itself – i.e., the computer code that encodes the logic which produced the decision. Unfortunately, algorithms are often proprietary and thus secret. This lack of transparency represents an important constraint on algorithmic accountability as the ability to evaluate the reasoning and evidence that motivated a decision and, if necessary, to contest that reasoning and evidence is central to our conceptions of justice and due process. In particular, increases in algorithmic decision-making pose a risk of undermining public sector accountability, thereby threatening its legitimacy[30]

Transparency and accountability are important for many reasons, including practicality: decision-makers, even algorithmic ones, often make mistakes and without external scrutiny, these mistakes will go uncorrected. These mistakes often have serious consequences. For example, an algorithm used by the Government of the United Kingdom appears to have wrongly accused 7,000 students of cheating on a test, an accusation which resulted in their deportation (Baynes, 2018).

Intelligibility

One suggestion for how to improve algorithmic transparency and accountability is to require that algorithms be equipped with an "ethical flight recorder" (Lant, 2017). Like the flight recorder in a commercial airliner which is designed to provide investigators with information that will allow them to determine the reason for a crash, this instrument would provide a record of the reasons why an algorithm took a particular decision.

While this proposal sounds reasonable, it is actually quite controversial. This is because, in order for this instrument to be useful, if would need to account for a decision in a form that was intelligible to humans. Given that algorithms are already making decisions which even their creators cannot understand, this could be challenging (Coglianese and Lehr Forthcoming, p. 10).

Consider the case of Google's AlphaGo, a machine learning algorithm designed to play Go – a two player strategy game popular in East Asia. AlphaGo made history in 2015 by being the first computer program to defeat a professional human opponent (BBC News, 2016). Since then, the program has grown significantly more powerful and can no longer be defeated by human opponents. Interestingly, however, it is winning by using strange and unorthodox strategies that human players cannot understand (Chan, 2017).

The AlphaGo example is illustrative of the difficulties inherent in forcing algorithms to provide intelligible accounts of their decision-making. If an algorithm can produce superior results by using logic that is incomprehensible to humans, is requiring an algorithm to provide an explanation in a way that humans can understand justifiable, if doing so blocks access to some of the most transformative benefits that algorithmic decision-making offers (Weinberger, 2018)? Or, if requiring an algorithm to provide an explanation for its decision that is intelligible to a human will force the algorithm to make worse decisions, is it worth it (Weinberger, 2018)?

4.1.3. Analysis and Opportunities

The breadth of opportunities that exist for the development of AI suggest that there is a wide scope for standards to play a positive role in this area. In particular, our research identified two powerful opportunities for standards to help ensure that the benefits of greater adoption of AI are spread widely.

The "Lawnmower of justice"

As the development of AI is heavily dependent on access to large pools of training data, one of the best ways to govern AI will be to govern the data used to train it. As a result, an important opportunity for standards-based solutions to positively impact AI is to establish standards for the data used to train it. This opportunity is perhaps best demonstrated by an idea called the "lawnmower of justice."

[30] For example, in the aforementioned use of risk scores in bail and sentencing decisions, defendants and their attorneys were not provided with access to the logic or calculations that produced the risk scores.

The "lawnmower of justice" is the name given to a technique designed to address the problem discussed earlier in which anomalous individuals are marginalized by probabilistic AI decision-making that privileges individuals with "normal" characteristics. The technique involves "trimming" the hump in the middle of a normal distribution so that the weight of this core of concentrated data points is made less overwhelming. This rebalances the distribution so that the AI being trained on this data learns to pay more attention to the outlying data points and the anomalous individuals they represent. The major drawback of this technique is that teaching the AI requires more data because it is not able to use the data that has been trimmed off. Consequently, the training process is slower and more costly. Positively, it also results in algorithms that are better able to respond safely and appropriately across more diverse sets of scenarios (Treviranus, 2018).

Figure 6 – *The Lawnmower of Justice*

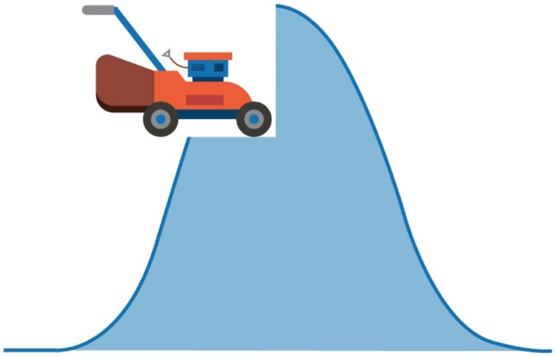


Image inspired by Treviranus (2018). Original image subject to an Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Creative Commons Licence https://creativecommons.org/licenses/by-nc/4.0/

Standardization of this technique could provide an important tool for ensuring that algorithms are not prone to the sorts of biases against small minorities described earlier. This approach could also form part of a wider algorithm development standard which could be used to identify algorithms trained using a suite of best practices.

Algorithmic transparency for public use algorithms

While transparency and accountability is important for protecting against bias in all contexts, they are especially important when governments and other public organizations use algorithms to assist in their decision-making where their use engages concerns regarding human rights, due process and the rule of law. The risk score and predictive policing algorithms discussed earlier are particularly concerning because of the power exercised by public bodies such as the ability to deprive individuals of their freedom.

Concerns of this type have been growing around the world. The City of New York recently created a special task force to review the use of algorithms by the city government and develop recommendations on "which types of algorithms should be regulated, how private citizens can 'meaningfully assess' the algorithms' functions and gain an explanation of decisions that affect them personally, and how the government can address 'instances in which a person is harmed' by algorithmic bias" as well as ways to make "technical information… publicly available where appropriate." The task force, which includes "individuals that are affected by algorithms, technology ethicists, city department heads using AI, technology companies as well as legal experts" will report in late 2019 (Powles, 2017).[31]

Addressing this nexus of concerns represents an opportunity for standards-based solutions. Despite some skeptical analyses, there may be ways to make algorithmic decision-making sufficiently transparent while still enabling firms to keep their source code secret. For instance, some scholars argue that governments can employ algorithmic decision-making if they:

1. Provide notice to individuals when government is using algorithmic decision-making in a way that might have a significant impact on them (Coglianese and Lehr Forthcoming, p. 24)[32]
2. Disclose the algorithm's outcome variable of interest and the objective function that the algorithm is designed to optimize (Coglianese and Lehr Forthcoming, p. 32)

[31] The text of the bill can be found here: https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0

[32] It should be noted that this would not cover banal and uncontroversial instances of algorithmic decision-making such as the post office's use of machine-learning algorithms to "read" handwritten postal codes on envelopes.

"Despite some skeptical analyses, there may be ways to make algorithmic decision-making sufficiently transparent while still enabling firms to keep their source code secret."

3. Provide evidence that the algorithm is sufficiently accurate to justify its use. This would include providing:
    a. individuals subject to the algorithm's decision-making with opportunities to inspect the data about them being used for accuracy
    b. a statement of the general accuracy of the algorithm's predictions
    c. the results of the verification procedures done to ensure that the algorithm was correctly implemented (Coglianese and Lehr Forthcoming, p. 33-34)

Even if algorithmic transparency and accountability are possible, many of the uses of algorithms to date by governments and other public bodies have not met the standards just outlined. For instance, the use of proprietary algorithms to rate teachers, largely on the basis of their students' scores on standardized tests, and then terminate the employment of the "lowest-performing" teachers on that basis, has stirred controversy and does not appear to have met these standards. In particular, it is not clear that any evidence, other than the algorithm's own conclusions, has been presented that those teachers identified as "bad teachers" were worse than the ones identified by the algorithm as "good teachers" (O'Neil 2017, Introduction).

Research already exists upon which SDOs could draw in developing standards for the use of algorithmic decision-making. For instance, a 2018 report focused on algorithmic decision-making in Canada's immigration system includes a detailed program of transparency and oversight measures that the authors argue ought to be implemented by the Canadian government in its use of algorithmic decision-making in its immigration application processes (Molnar and Gill, 2018). This analysis, and others like it, provide a strong basis for the creation of standards as well as programs for the accreditation of institutions against these standards. While the focus would likely be on public institutions initially, similar standards will also be needed for the private sector, especially for platform firms that already perform significant governance functions for their users.

4.2. Algorithmic pricing

Increasingly, firms are using algorithms to dynamically set prices. These algorithms use a variety of inputs ranging from a user's postal code, their browsing history and even the users' predicted emotional state. The increasing use of these algorithms, and their growing capabilities, are raising concerns as many perceive them as having the ability to manipulate consumers and potentially damage the larger economy.

4.2.1. Current governance landscape

Dynamic pricing refers to the practice of offering an "identical/similar product or service to different customers (or groups of consumers) at different prices" (Deane 2017, p. 12). Dynamic pricing is not new. Airlines, for example, have long varied the prices of flights on the basis of a range of factors. But it is only recently, thanks to the migration of an increasing proportion of commercial transactions online, that the ubiquitous use of algorithmically-controlled dynamic pricing has emerged. This novelty may be one of the reasons why there are so few governance instruments in this area. Indeed, in a report published in 2017, researchers found no applicable international standards "substantively addressing dynamic pricing and its processes" (Deane 2017, p. 9)

One area where algorithmic pricing has garnered significant attention is in its use by ride-sourcing firms. Uber's "surge" pricing, an algorithmic pricing model designed to better match the supply and demand for rides through fare increases during times of high demand, is likely the most notorious use of algorithmic pricing. Unsurprisingly, surge pricing is also responsible for some of the few governance instruments that have been developed specifically for this area. For example, in response to public criticism over the activation of "surge" pricing during Hurricane Sandy and pressure from the Attorney General of New York, Uber agreed in 2014 to cap its price increases during emergencies in the USA (Popper, 2014).

When limits on dynamic pricing are discussed, the focus is usually on how dynamic pricing can lead to price gouging. But algorithmic pricing could also potentially result in prices that are too low. In fact, concerns over "predatory pricing" have motivated a major area of law applicable to algorithmic pricing, namely competition law. In Canada, predatory pricing, defined in the Competition Act as "selling articles at a price lower than the acquisition cost for the purpose of disciplining or eliminating a competitor" can constitute a prohibited abuse of a dominant position.[33]

4.2.2. Challenges

Dynamic pricing is often defended on the grounds that it can encourage the emergence of a more productive economy because of how it can more efficiently match supply with demand. Algorithmic pricing offers this benefit and more: by making use of Big Data, algorithmic pricing can enable sellers to price goods and services in ways that are much more responsive and targeted to individual consumers.

In theory, this could result in firms competing vigorously for every single customer on the basis of their individual wants, resources and willingness to pay. For a variety of reasons, some of which are discussed below, this consumers' paradise has not emerged.

Personalized pricing

The most obvious challenge presented by algorithmic pricing can best be described as "personalized pricing." Personalized pricing involves sellers differentiating the prices they offer not only on the basis of contextual factors like the prevailing balance between supply and demand, but also on information about – or inferred about – the characteristics of individual customers (Deane 2017, p. 12).

There are already some well-known forms of semi-personalized pricing such as senior or student discounts. Given the popularity of these discounts, it may seem odd to identify personalized pricing as a challenge, especially for consumers. But there are critical differences between these forms of static personalized pricing and the more dynamic types which Big Data and AI enable.

For instance, unlike existing semi-personalized pricing, the most likely outcome of widespread personalized pricing will likely be that algorithms will get better at finding ways to get everyone to buy or pay more. This could happen in a number of ways. First, by eliminating benchmark "reference" prices by personalizing prices for more and more transactions, algorithmic pricing will make comparison shopping more difficult. For example, consumers may not be able to rely on recommendations from family or friends because they will likely be offered different prices. Second, algorithms will get better at identifying prices that are just below the price that would make it worthwhile for a consumer to look elsewhere for a better one. Finally, algorithms will get better at determining when customers are pressed for time or are under duress and then exploit these moments.[34]

[33] See sections 78 and 79 of The Competition Act http://canlii.ca/t/7vdv

[34] Consider the, albeit extreme, example set by Uber's use of surge pricing during a mass shooting and hostage taking incident in Sydney, Australia (BBC News, 2014).

The elimination of a benchmark price has anti-competitive implications which are discussed further below. But it is also worth discussing the implications of the ability to predict consumers' behaviours that underlie the second and third of these examples. The idea that an algorithm will be able to predict consumers' behaviour with this level of accuracy may seem far-fetched; it is not. Some firms have actually already started to steer consumers into different pricing "aisles" online by offering those using Apple devices higher prices, on the assumption that they have a greater willingness to spend, than those with Android devices (Deane 2017, p. 15). Now consider how much more accurate these sorts of pricing strategies will become under the control of an algorithm that, once it has accumulated sufficient data points from a customer, may be better able to predict that customer's behaviour than any human being could (Youyou et al., 2015).

More concerning is the fact that firms may also begin acting in ways that pass from prediction into manipulation. For example, some firms have already demonstrated their ability to manipulate users' emotional states (Rose-Stockwell, 2018). In fact, there are already well-established approaches to designing and marketing digital products and services which seek to modify users' behaviour through "persuasive design" (Lewis, 2017).

Undetectable predatory pricing

Another important challenge presented by algorithmic pricing is that it may enable dominant firms to engage in predatory pricing more effectively than was previously possible. In the past, predatory pricing would have required firms to physically discover their competitors' prices by visiting stores or reading catalogues before adjusting their own prices. Now, digital firms are able to use algorithms to continuously check their competitors' prices online and adjust their prices accordingly.[35] As one scholar notes, this is even easier for platform firms like Amazon where the firm, which in addition to providing an online marketplace for third party sellers also sells its own goods in the same marketplace, is able to monitor its competitors' prices through its own platform infrastructure (Khan 2017, p. 782-783).

To a certain extent, this sort of price competition will be welcomed by consumers as it could result in lower prices, at least in the short term. But over the long term, these new capabilities could have serious anti-competitive impacts. If dominant firms are able to more easily drive competitors out of the market, and in so doing credibly signal that they will pay the price necessary to do so in the future, they will be better able to establish monopolistic positions with nothing to stop them from raising prices over time.

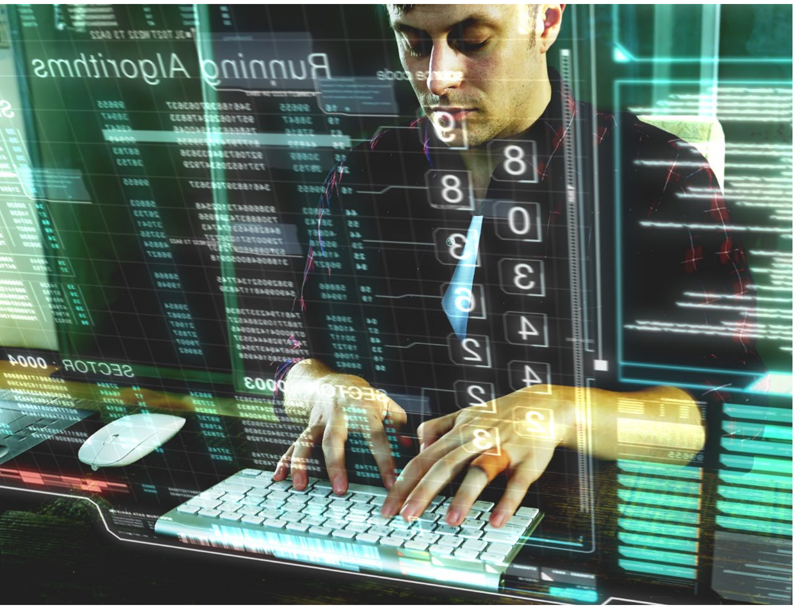
Algorithmic pricing may also make this behaviour difficult for regulators to identify. The ability to gather price information from the entire Internet and instantaneously adjust prices, combined with the price opacity of personalized pricing and the attendant loss of "benchmark prices," may render predatory pricing almost undetectable (Khan 2017, p. 762-63). Should this occur, competition authorities may be left powerless to arrest the creeping monopolization of large sectors of the digital economy.

Tacit collusion

Algorithmic pricing may also enable an opposite but equally concerning outcome, namely, tacit collusion. In this scenario, firms' pricing algorithms may conclude that the most profitable approach is to stop competing on price and gradually raise prices in parallel over time. While such an approach would be illegal if it were designed by humans who agreed to it as a means of cartelizing a market, such tacit collusion would likely not be illegal under existing law if it were independently implemented by multiple pricing algorithms that did not engage in explicit communications with each other.

What makes this especially worrying is that non-digital instances of tacit collusion have already been well-documented and the characteristics of these situations which allowed tacit collusion to emerge will likely define many digital marketplaces. For instance, in multiple countries, tacit collusion has arisen in markets dominated by a small number of firms which have easy access to updated information about each other's prices.

[35] See https://www.practicalecommerce.com/Monitor-Competitor-Prices-with-Python-and-Scrapy for an example.



"One of the major problems with algorithms is that they are often deployed before they have been rigorously tested."

Through experimentation and the sending of signals through their prices, firms have been able to engage in parallel price increasing strategies, thereby enabling them to increase profits at the expense of consumers (Stucke and Ezrachi 2017, 9-13).

In a digital context, it could be even easier for pricing algorithms to monitor competitors' prices and respond to any changes by varying their own prices almost instantaneously. This should provide profit-maximizing algorithms with an optimal environment in which to learn both that collusion is the best way to increase profits and how to collude tacitly – all without human direction. Because this could be done without communication, or even any human intention to collude, it is unlikely that this behaviour would be illegal under existing laws (Ezrachi and Stucke 2016, p. 66). And even if the law was changed to prohibit tacit collusion, it is not clear how it would be possible to prove it was actually taking place.

4.2.3. Analysis and Opportunities

Overall, there are only a few opportunities for standards-based solutions to play a major role in governing algorithmic pricing. Nonetheless, there are some, though progress in certain areas may first require further technological developments to enable more direct governance measures.

Transparency standards for pricing algorithms

One of the major problems with algorithms is that they are often deployed before they have been rigorously tested (Angwin et al., 2016). While governments and regulators may eventually develop the capacity needed to set rules for how algorithms engage in activities like pricing – and test them for compliance – they currently do not possess this capacity.[36] This leaves SDOs with an opportunity to generate standards for the use of these algorithms and develop procedures and techniques for testing pricing algorithms, to determine if they are likely to engage in problematic practices like predatory pricing or tacit collusion.

The Consumers Council of Canada has already recommended that SDOs consider developing a standard for dynamic pricing. This recommendation could be extended to providing "principles and guidance in designing, developing, implementing, maintaining and improving an open and honest relationship with consumers" for firms using algorithmic pricing (Deane 2017, p. 10). Such a standard could include measures designed to extend the concepts of notice, access and informed meaningful consent to the use of personal data by firms' pricing algorithms (Deane 2017, p. 10). These standards could take inspiration from California's aforementioned *Consumer Privacy Act* which focuses on

[36] One promising area where progress may be coming is in the use of "formal methods" for evaluating computer code (The Economist, 8 April, 2017b).

providing consumers with a choice over whether their personal data is collected and used by firms. They could also include protections of the concept of a common reference price against the relativism of constantly shifting prices and prohibitions against anti-competitive actions such as predatory pricing and tacit collusion.

"Incubators" for pricing algorithms

Were such standards established, certain additional steps would be needed in order to make them practically useful. Specifically, prohibitions against predatory pricing and tacit collusion would require means of certifying algorithms' compliance with these prohibitions. As discussed earlier, determining how a particular algorithm will act, or explaining its decision-making, can be difficult. This reality, combined with firms' general unwillingness to allow outsiders to inspect their algorithms' source codes, suggests that the optimal way of certifying an algorithm's compliance with a particular condition is to test it.

Testing an algorithm could involve developing an "incubator" or controlled information environment. In this environment, the algorithm would be exposed to a series of fictitious market scenarios designed to test the algorithm's response to a host of competitive scenarios. Specifically, the algorithm would be provided with opportunities to profit by engaging in predatory pricing or tacit collusion (Stucke and Ezrachi 2017, p. 43-53). Algorithms that successfully avoided engaging in these prohibited behaviours would be recognized potentially with a certification.[37]

5 Digital platforms

The rise to prominence of digital platforms has been a key feature of the digital revolution. From the increasingly dominant GAFA (Google, Amazon, Facebook and Apple) to hard charging unicorns like Uber and Airbnb,[38] to older firms like Microsoft and Netflix, almost all of the most successful digital firms depend in important ways on their digital platforms.

Digital platforms are responsible for a significant proportion of the positive contributions that have been delivered so far by the emergence of the digital economy. Not only have they significantly lowered "transaction costs,"[39] thus making many tasks easier and more economical, in so doing they have enabled whole new markets to emerge online, such as short-term accommodation. Simultaneously, however, the emergence of digital platforms has also produced a number of worrying tendencies. For example, digital platforms are often characterized by high "switching costs" – the cost of moving one's activities from one platform to another – which can make markets less competitive.

Through an examination of the structural issues which characterize digital platforms, and a more focused examination of digital labour platforms, this section examines some of the most important ways in which digital platforms and their effects are having an impact on the wider digital economy.

5.1. Structural issues

Many digital platforms have been successful because of their ability to exploit a few key features inherent to the platform business model such as "network effects." Network effects are a phenomenon whereby the value of a product or service, such as a marketplace, is influenced by the extent to which it is used by others. The more sellers that are active in the marketplace, the greater the variety of goods and prices offered is likely to be, which in turn makes the marketplace more attractive to buyers. As the marketplace draws more buyers, this in turn attracts more sellers who want to be where potential customers are.

Network effects are not necessarily bad. The reason that a popular online marketplace draws many buyers and sellers is because it is useful to them. But when a new technology or business model emerges, the accompanying shifts in economic activity also expose weaknesses in the existing governance frameworks.

[37] Analogous efforts aimed at developing processes for certifying algorithms as meeting certain ethical standards are already underway. See https://standards.ieee.org/industry-connections/ecpais.html

[38] The term "unicorn" refers to a privately held start-up company that is worth more than a billion dollars.

[39] Transactions costs refer to the costs involved in finding a counterparty in a market, bargaining with them and monitoring/enforcing agreements with them.

These structural issues, which were not considered or protected against in the past, often require compensatory governance frameworks.

5.1.1. Current governance landscape

There are few existing instruments, or instruments in development, that seek to respond to the emergence of specific structural issues related to digital platforms. While legislation such as GDPR have focused on aspects such as privacy and consent, standards for platform design are lacking.

While traditional rule instruments are generally lacking in this area, some softer initiatives are worth highlighting. Many of these initiatives are aimed at helping users make informed decisions online, for example, by providing evaluations of various ToS agreements. Creative Commons' "human readable" versions of software licenses, the "Terms of Service; Didn't read (TOS;DR)" project, and watchdog project FairCrowdWork.org's assessment of the ToS of crowdwork platforms are all examples of initiatives that seek to provide easy-to-read summaries and ratings for the ToS of major websites and Internet services.[40]

5.1.2. Challenges

As discussed earlier, traditional governance frameworks are often inadequate for the digital context. Solving the structural issues generated by the emergence of digital platforms requires understanding the unique nature of many of the challenges involved in their design and architecture.

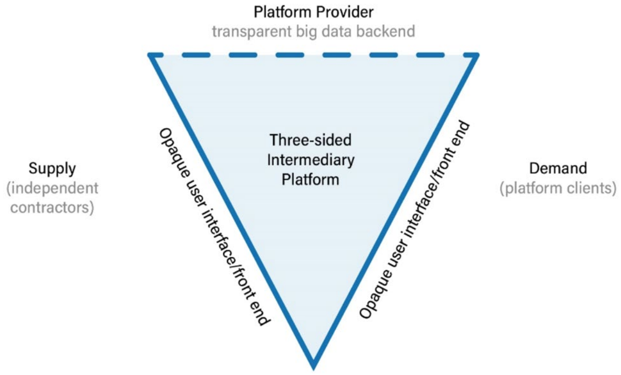
Information asymmetry

While digital platforms often suggest that they only serve as intermediaries that enable buyers and sellers to discover and connect with each other, a closer look at their architectures and business models reveals that they do much more. Indeed, while economic activity on digital platforms is often described as unregulated, it is actually "platform-regulated" with platforms exercising significant power in setting the terms of interaction compared to other stakeholders (Berg 2016, p. 25).[41]

The scope of this platform regulation is significant. Digital platforms set the terms of interaction and governance, facilitate compensation and control or influence the interactions or transactions that take place on the platform. They also decide what and how information is collected and displayed, who is able to interact with whom, and how disputes are mediated and resolved. Additionally, platforms control which parties (service providers, consumers and clients) see what information, and can influence their interactions, often in real-time. This creates systematic information and power asymmetries which favour platform interests over user interests (Schmidt 2017, p. 10),[42] a problem that is exacerbated by the fact that most users are not even aware that the platform controls what they see (Smith, 2018).

In many cases, information asymmetry is deliberately created by platforms to protect their interests against users making optimal decisions for themselves. In the case of ride-sourcing platform Uber, for instance, the app withholds key information from the driver, such as the destination and fare, until after the driver has accepted the ride. Drivers are also penalized if they cancel a ride after learning these details. This system has increased acceptance rates and reduced cancellations – thereby helping Uber's business, while reducing drivers' freedom of choice (Choudary 2018, p. 10-11).

Figure 7 – *Three-sided Platform Architecture*


Platform Provider
transparent big data backend
Three-sided Intermediary Platform
Supply (independent contractors)
Demand (platform clients)
Opaque user interface/front end
Opaque user interface/front end

Source: Schmidt (2017, p 10).

[40] Crowdwork refers to tasks, usually quite small and simple in nature though often completed in large volumes, completed through online platforms such as Amazon Mechanical Turk and Crowdsource.

[41] See Ezrachi and Stucke (2016, p. 178-190) for a discussion of how platforms like Apple's App Store and Google's Play Store apply their own standards to the apps that are sold there.

[42] For example, platforms like YouTube and Twitter, which make more money the longer users stay on their sites, are being criticized for driving greater user engagement by privileging emotionally engaging, but often misleading, content (Friedersdorf, 2018 and Meyer, 2018).

Digital platforms also often actively determine who can provide services by, for example, setting training requirements or evaluating workers through peer-review systems. Some crowdwork platforms also charge clients fees to get access to "better" workers. Communication between workers and clients is generally restricted and controlled by platforms to make it difficult for workers and clients to connect independently (Berg 2016, p. 21).

Skewed ToS

Digital platforms' use of "clickwrap" ToS agreements, which users of digital services like apps and websites are required to accept without negotiation before they are allowed to use the services, have created another significant imbalance. Combined with the concentrated market power produced by network effects and high switching costs, unbalanced ToS have helped create a digital economy where users' interests are routinely marginalized in favour of platforms' interests.

First, platforms use ToS to give themselves broad permission to organize their businesses in ways that are advantageous to them. While users only need to click "accept" when agreeing to an entire ToS agreement, should they want to opt out of even a small part, such as waiving their right to participate in a class action lawsuit, they are required to make disproportionate efforts such as "sending notice in writing within 45 days by first class, certified mail, or overnight courier" (Stinson, 2018). Platforms also tend to absolve themselves of as much liability as possible, often transferring it to users (Schmidt 2017, p. 11). For example, many labour platforms' ToS require workers to waive legal rights, including the right to trial or to participate in a class action lawsuit as a means of resolving a dispute with the platform (Berg et al. 2018, p. 105).[43]

ToS are also designed to push users to accept them without reading or understanding what they are agreeing to, mainly due to the sheer volume of text and the complexity of the legal jargon in which they are written. Research by the International Labour Organization (ILO) on crowdworking platforms found that platforms' ToS are lengthy (generally over 10,000 words) and difficult to understand (Schmidt 2017, p. 11).[44] Moreover, ToS usually include clauses which allow platforms to change the contents of the agreements at any time without notice, further reducing users' incentives to read them. ToS are also one-sided in that they often ignore issues of importance to users and do not allow users to negotiate the agreement's terms with platforms. The only choice available is to agree, even if they are profoundly problematic, or not use the service (Berg et al. 2018, p. 22-23). This is especially problematic in the context of digital labour platforms where workers' access to the platform may be essential to their livelihoods.

Concentration of power

Digital platform business models, which create "winner take most" marketplaces, have been extremely successful for some firms. Google and Facebook, for example, are two firms that did not exist 25 years ago and are now some of the largest and most profitable companies on the planet. These profits have helped make these firms formidable competitors, but not always in ways that benefit consumers. For example, they have been regularly criticized for using their significant revenues to engage in numerous "shoot-out" acquisitions of start-ups, neutralizing the potential future competitive threat these smaller firms represent (The Economist, 2 June, 2018).[45]

As highlighted earlier, platforms firms often design their services so as to make switching to other platforms costly for users. They have largely done this through their control of the data that users generate on their platforms. Users who wish to move to a new platform are usually not able to download and transfer the data they have created on the first platform to a second one. Switching to a new platform means starting all over again from scratch. This is a major disincentive that discourages many users from switching platforms, especially if they depend on their work history or reputation data for their livelihoods, as might be the case with digital platform workers like crowdworkers, Uber drivers or Airbnb hosts.

[43] There has been some resistance to these practices. For example, the Ontario Court of Appeal recently ruled that that Uber's driver services agreement that requires drivers to resolve conflicts in the Netherlands is "unconscionable" and "invalid".

[44] Indeed, Airbnb's ToS are 55,000 words long.

[45] On average, Google and Facebook acquire about two other firms each month.

> *"Global platforms can often get away with violating local regulations or laws as these firms rarely have a local physical presence, making enforcement difficult."*

This creates dependency for users and also reduces competition amongst platforms (Choudary 2018, p. 4).

Ostensibly, the GDPR provides users the right to download any data concerning them held by the platform. But it is not clear yet whether this ability will be extended outside of Europe and whether the download formats will be sufficiently interoperable to allow true portability of data between services.[46] Moreover, while firms are required to make data available for download, they are not required to upload such data from users if they bring it from another platform.

Transnational nature

Digital platforms are often transnational in scope. For instance, crowdwork platforms enable workers to work remotely from anywhere, and on-demand location-based app companies are not necessarily based in the jurisdictions where they operate. This can make it difficult to determine which jurisdiction's laws should be applied, particularly when it comes to dispute resolution. Consequently, it is also not surprising that there are often clashes between platforms' ToS agreements and local laws (Schmidt 2017, p. 11).

This jurisdictional uncertainty creates risks for users, who may face penalties in such a scenario. Conversely, because of their ability to strategically base themselves in a legally friendly jurisdiction and hire high quality legal expertise, the risk for platforms in a dispute is often much lower (Choudary 2018, p. 13). Indeed, global platforms can often get away with violating local regulations or laws as these firms rarely have a local physical presence, making enforcement difficult. Uber's arguably illegal launch in many cities offers a good example of this.

The geographic dispersion of labour and the impersonal nature of digital work also makes it difficult for workers to organize collectively. In the case of crowdwork, where many workers from across the world compete for the same jobs, such solidarity becomes even more difficult as workers come from diverse countries and backgrounds with starkly different economic conditions, such as minimum wage and labour laws. This results in workers seeing each other as competition rather than colleagues, and also feeling powerless in negotiating wages because of fears that they could be easily replaced (Graham et al., 2017).

5.1.3. Analysis and Opportunities

The lack of rule instruments designed to address platforms' structural issues suggests that there may be opportunities for standards-based solutions in this area. Nonetheless, one of the likely reasons for this dearth of governance is the dominance of this space by powerful

[46] Uber is currently fighting a request from drivers for access to their data under the GDPR arguing that the partial disclosure that it has already provided is sufficient. The drivers argue that this partial disclosure of data is not sufficient (The Economist, 20 March, 2019). One area where data portability is more advanced is the "Open Banking" that has been enabled by the EU's Payment Services Directive – known as PSD2 – which has required European banks to share customer data with competitors if the customer requests it. It has been most successful in the United Kingdom where regulators and industry groups have started to build the infrastructure needed to enable fuller data portability, such as standardized formats and coding languages for application program interfaces (APIs) – the technology which enables this portability (Thomas et al., 2019).

interests that prefer to set their own rules. Efforts to create new rule instruments will need to take this into consideration.

User-Friendly ToS

As mentioned earlier, there are opportunities to develop standards for ToS agreements, building on existing rule instruments like the EU's GDPR and California's *Consumer Privacy Act.* Beyond the already discussed focus on data collection and use, a comprehensive digital platform standard for ToS agreements could include terms related to:

- Meaningful consent.
- Accessibility and intelligibility for non-expert users.
- Ability to decline platform requests for data that are not necessary to the use of the platform, without being barred from using the platform.
- Opt-out provisions that are no more difficult to exercise than the procedures for consenting to requests from the platform.
- Expiry of consent and procedures for renewing consent, particularly if ToS are modified.
- Not requiring waiver of legal rights to access dispute resolution mechanisms like courts.

Standards for platform interoperability

According to research from the ILO, a governance framework for digital platform design should take into account the following considerations:

- Decrease information asymmetry to increase workers' bargaining power.
- Reduce worker dependency on platform-controlled proprietary data (e.g. reputation data).
- Rethink data ownership (Choudary 2018, p. 34-35).

Currently, platforms either own or give themselves broad rights to exploit users' data through their ToS. This allows platforms to control users' data for a variety of purposes including the ability to understand and influence behaviours. To reduce the power asymmetries between users and platforms that this creates, users' control over their own data needs to be better developed (Choudary 2018, p. 34-35). One important step that could be taken in this direction is to enable greater transparency.

The way in which work history and reputation data is handled provides a good example of what greater transparency in platform design might look like. By creating standards for platforms' peer-review and ratings systems, SDOs could create comparability in this data and enable their transfer across platforms. Doing so would be critical to giving individuals greater control over data concerning them. For example, digital platform workers like Uber drivers cannot transfer their five-star rating data and use it on other platforms. By creating a common standard for such rating information, SDOs could neutralize an important potential excuse for resisting data portability and, in so doing, promote worker mobility and competition between platforms, as well as help to enable new decentralized digital business models.

5.2. Digital labour platforms

In the past two decades, and especially in the years since the start of the Financial Crisis, a host of digital labour platforms have emerged and gained significant popularity by providing workers with opportunities to earn income through "gig" work.

Gig work generally includes freelancing, crowdwork and work-on-demand through apps, such as Uber and Lyft. Freelancing on digital platforms is similar to traditional freelancing except that the medium through which freelancers advertise and are contacted has shifted to digital platforms. On-demand work includes traditional jobs such as transportation, cleaning and handyman services that are managed by apps that match supply and demand, and also often set minimum standards for service (Berg 2016, p. 1).

For many workers, this sort of work is becoming their main source of income. A 2017 ILO survey found that crowdwork was the primary source of income for 32 per cent of the workers on crowdwork platforms (Berg et al. 2018, p. xvii). A survey of on-demand service economy workers in the Greater Toronto Area found that about half of these workers (48 per cent) had been engaged in such work for over a year – indicating that for many, these jobs are important sources of ongoing employment rather than temporary "gigs." Many desire more stable employment – 53 per cent say that they are only engaging in gig work until they find something better, while 55 per cent say that gig work is the only way for them to make money (Block and Hennessy 2017, p. 5-7).

5.2.1. Current governance landscape

Broadly speaking, no formal labour laws have been specifically designed for this new model of employment in Canada. Indeed, policymakers across the world are grappling with the precarious employment that is often facilitated by digital platforms, as traditional employment laws, regulations and standards are largely inadequate to respond to the novel challenges presented by digital labour platforms.

The existing governance framework begins with the system of international labour standards that the ILO has maintained since 1919.[47] In Canada, federal labour standards were established in the 1960s and have remained relatively unchanged since that time (What We Heard 2018, p. 1). Given the rise of non-standard work in recent years, these labour standards are in need of updating as many workers lack protections and face economic vulnerability. Indeed, when the Canadian government conducted consultations in 2017-2018, the idea that labour standards need to catch up with changing employment conditions, particularly in the face of technological disruption and global competition, found wide support (What We Heard 2018, p. 2).

In response to changes in the nature of work, several initiatives are currently underway. The ILO has launched a "Future of Work initiative" to respond to new challenges and advance social justice.[48] In February 2019, the Government of Canada launched an independent panel to provide recommendations on how to address issues facing Canadians in the workplace, including potential updates to labour standards, protections for non-standard workers, collective voice for non-unionized workers and portable benefits.[49]

In Germany, a "Crowdsourcing Code of Conduct" was developed in 2015 by the German software testing platform Testbirds. This code included principles such as fair payment, only serious tasks and open and transparent communication. An Ombuds office was established in 2017 to enforce the code and resolve disputes between workers and platforms. Managed by IG Metall, this office comprises a board of five people – one worker, one trade union representative, one platform employee, one Crowdsourcing Association representative and a neutral chair, who come together to resolve disputes (Berg et al. 2018, p. 99).

While not aimed specifically at digital platform workers, the "10 Principles for Workers' Data Rights and Privacy" developed by the UNI Global Union provides a similarly useful foundation for future rule instruments focused on workers' rights in an increasingly digitized employment landscape.[50]

There are also some existing standards-based solutions which apply directly to platform work. For example, IWA 27:2017 *Guiding principles and framework for the sharing economy* seeks to provide high-level principles that can act as a foundation for governance of the sharing economy.[51] These principles are of interest because most sharing economy operations are carried out via digital platforms. ISO has formed a technical committee, ISO/TC 324, that is working to develop standards related to the sharing economy.[52] Work to develop best practices for municipalities on the basis of this IWA is also currently being carried out by CSA Group (Alwani and Urban, 2019).

Finally, the UK sharing economy TrustSeal is the world's first kitemark for sharing economy companies and was created by Sharing Economy UK, an industry association for sharing economy organizations in the United Kingdom. To be granted the TrustSeal, organizations must undergo an assessment process which includes evaluation of the adherence of sharing economy platforms to a set of six principles of good practice.[53] While not primarily focused on labour standards, the TrustSeal does cover some areas of interest to workers such as peer reviews. The process by which firms are certified could provide a model for certification of adherence to digital labour standards.

[47] See https://www.ilo.org/global/standards/introduction-to-international-labour-standards/lang--en/index.htm

[48] See https://www.ilo.org/global/topics/future-of-work/lang--en/index.htm

[49] See https://www.canada.ca/en/employment-social-development/news/2019/02/expert-panel-to-provide-advice-on-complex-workplace-issues-facing-canadians.html

[50] For more information, see http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf

[51] See https://www.iso.org/news/ref2225.html

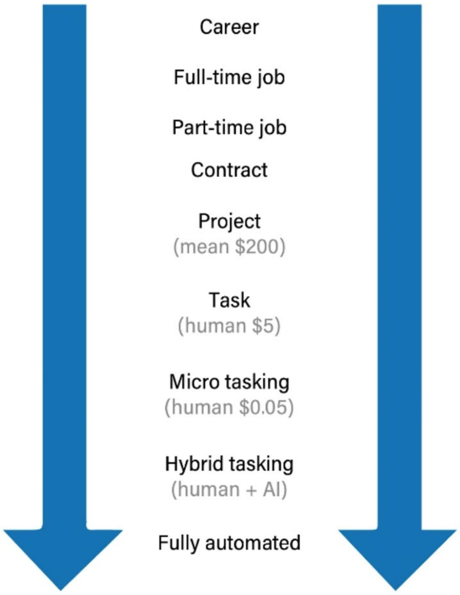
[52] See https://www.iso.org/committee/7314327.html

[53] See: http://www.sharingeconomyuk.com/trustseal

5.2.2. Challenges

While digital platforms tend to increase the convenience with which users can access goods and services, the efficiency of the markets that they create also tends to encourage the unbundling of work and the commodification of labour (See Figure 8). This commodification – meaning that competition amongst providers occurs on price and not on quality – raises important challenges as it impacts people's livelihoods directly and can be especially problematic for those already in precarious positions.

Figure 8 *– The Progressive Unbundling of Work*



Source: Policy Horizons. (2016). Canada and the Changing Nature of Work. Ottawa: Government of Canada. Page 2.

Non-standard employment relationship

While often celebrated for providing workers with new opportunities to earn income more flexibly, the gig economy is also criticized for lacking effective labour standards and for creating working conditions that are often unstable or unsafe. To a great extent, this is the result of the employment status of digital platform workers.

On most digital labour platforms, workers are classified as "independent contractors" or "self-employed." Platforms defend this classification by pointing out that they serve as intermediaries that connect service providers or workers to customers or clients.

Not operating within a standard employment relationship typically means that many national labour laws are not applicable to digital platform workers. These non-standard workers rarely receive employment protections or benefits from platforms or clients, and their right to collective bargaining is often not recognized. In Ontario, for example, such workers are excluded from the Employment Standards Act, meaning that they are not eligible for protections such as overtime pay or minimum wage. Additionally, in non-standard relationships, the liability for unforeseen circumstances is often passed on to workers. For example, the cost of insurance is generally borne by workers in ride-sourcing services like Uber. Even more worrisome is the fact that since platforms' ToS agreements are often so lengthy and difficult to understand, workers often unwittingly take on risks for which they are not insured (Choudary 2018, p. 13).

In addition to not receiving the benefits associated with standard employment relationships, digital platform workers also often miss out on the freedoms usually associated with self-employment. For example, crowdworkers are often penalized for not accepting work, are not allowed to sub-contract and are not permitted to use bots, scripts or AI algorithms in their work. Many freelance workers are required to transfer all intellectual property rights for their work to the client once it is submitted, even if it is rejected by the client (Berg et al. 2018, p. 104-105). Similarly, platforms, such as Uber, Lyft and Deliveroo, do not allow workers to bargain over pay, either with the platforms or the customers. Transportation platforms also often determine the routes that the drivers must follow. Deliveroo requires its couriers to work at least two of three evenings between Friday and Sunday, and creates schedules for couriers which they must accept a week in advance (Choudary 2018, p. 17).

"Worker-led cooperative enterprises have recently begun to emerge as alternatives to centralized corporate-operated platforms."

Social protections and compensation

One of the most visible challenges related to digital labour platforms is their link to increases in precarious employment. "Precarious employment" generally refers to work that is low paid, unstable, and lacks social protections such as medical benefits and pension plans (Noack and Vosko 2011, p. 14) – all features of many forms of digital platform work. Often, workers in precarious situations also face threats to their health and safety. While many workers on digital platforms enjoy the flexibility to set their own work hours or work from home, digital platform business models tend not to prioritize decent work and wellbeing of workers – particularly for those workers who are unable to find standard jobs and must rely on digital platform work for their livelihoods (Field and Forsey, 2016).

The situation of digital food delivery platform workers in Ontario offers a good example of both the unevenness of the digital platform employment landscape and the way in which digital platform workers can be disadvantaged by their employment status. In a recent investigation of three food delivery apps active in Ontario – Uber Eats, SkipTheDishes and Foodora – CBC's Marketplace found that only Foodora pays into the province's work-related compensation system (Ghebreslassie et al., 2018). While Ontario's Workplace Safety and Insurance Board (WSIB) provides automatic coverage to couriers who deliver services by bike or on foot, and all companies employing them must pay into the system, Uber Eats was not registered with the WSIB at all, with the company arguing that delivery couriers are independent contractors, not employees of the company (Ghebreslassie et al., 2018).

Low pay is another common characteristic of digital platform employment. Currently, many crowdwork platforms do not provide any guidelines for price setting (Berg 2016, p. 21). An ILO survey of crowdworkers found that depending on the country, crowdworkers earn between $1.00 and $5.50 per hour. This was a recurring complaint from workers who participated in the survey, and ranked increased pay as a key factor in increasing job satisfaction. Many workers suggested that tasks should pay at least minimum wage (Berg 2016, p. 11-12).

Not only is compensation for digital workers lower, they also tend to be marginalized compared to consumers or clients on the platforms. For example, if a passenger forgets a belonging in an Uber, Uber requires the driver to return the item without being compensated for their time. On Amazon Mechanical Turk, if a client is unsatisfied with the work, they can decline payment, but are allowed to keep and use the work. On UpWork, workers often bid in a competitive auction-style system which encourages them to lower their wages significantly. On 99Designs, many designers work on the same brief, but only the winning design gets paid (Choudary 2018, p. 15-16). Many other platforms also let clients launch competitions which result in multiple workers working simultaneously on the same task. Clients then select and pay for only the product they like best (Berg 2016, p. 3).

In the gig economy, workers often work on tasks that do not require specialized skills or education, such as in ride-sourcing or food delivery. Most "microwork" performed on platforms includes simple and repetitive tasks, such as filling out surveys, accessing content on websites, transcription etc. (Berg et al. 2018, xviii). As a result of this commodification, platforms often prioritize the growth of their network over managing the concerns of existing workers who are deemed replaceable. Correspondingly, platforms are relatively uninterested in working to retain workers by providing attractive pay or benefits. It also means that low-skilled workers without permanent jobs – who often rely on these platforms as their primary source of income – are put in even more precarious situations (Choudary 2018, p. 15).

Lack of mechanisms for dispute resolution and redress

Digital labour platforms have generally been poor in their provision of dispute resolution mechanisms for workers. In one survey, 38 per cent of respondents identified customer disputes as an issue and 20 per cent said dealing with platform firms was difficult (Block and Hennessy 2017, p. 5-7). In particular, many platforms rely on five-star rating systems where service providers and customers rate one another. While this can serve as a useful tool for encouraging quality service and gauging performance, it can also be detrimental for workers who unfairly receive lower ratings with no adequate means to contest these ratings (Ince, 2017). This is problematic as these ratings are often critical to workers' ability to secure future gigs and can even form the basis for being banned from the platform. Moreover, for crowdwork platforms, rating systems are often one-sided with platforms lacking mechanisms for workers to rate clients.

One of the main sources of disputes between workers and clients is work rejection and clients' refusal to pay for work. An ILO survey found that 94 per cent of crowdworkers had had their work rejected or had been refused payment. Such rejection and non-payment can occur even when the work is still useful to the client who often gets to keep the rejected work (Berg et al. 2018, p. 73-78). In many cases, the platforms involved were unresponsive to these concerns and provided no adequate means for dispute resolution (Berg 2016, p. 13). In fact, platforms' ToS often allow clients to refuse payment for the work if it is deemed unsatisfactory without providing a rationale, while still being able to retain that work as well as the associated intellectual property rights. Such provisions can enable wage theft from workers and negatively impact their ability to secure other work (Berg 2016, p. 14).

A critical factor that contributes to these problems is the opaque "black box" character of the algorithms that are often used by clients to review work. Because of this, clients themselves are often unable to explain why the task was rejected. Thus, in addition to not being paid, workers cannot obtain feedback explaining why their work was rejected, limiting their ability to improve their work. Such a system, meant to run on autopilot through algorithmic management, significantly disadvantages workers. Moreover, platforms favour clients over workers: platforms generally do not require clients to respond to complaints, while workers are often banned if they receive too many rejections without any explanation. Finally, since thousands of microworkers often work on the same tasks for large clients, the cost for the client to respond to an individual is often greater than the amount the worker is being paid. Similarly, for workers, following up on unpaid microtasks can take more time than the task itself, which makes seeking redress difficult to justify financially (Berg et al. 2018, p. 73-78).

Discrimination

While remote work can reduce discrimination by providing anonymity to digital workers and increasing access to work for people who are homebound due to disability or other health issues, discrimination can still occur. In fact, new forms of discrimination have emerged. For example, clients can often limit the geographic areas where the worker must be based in order to be eligible for a task, rather than set objective criteria such as language proficiency (Berg 2016, p. 11).

Similarly, on-demand platforms have also been accused of enabling discrimination based on factors such as race or socioeconomic status. In the case of ride-sourcing firms such as Uber and Lyft, passengers may cancel rides based on the race or ethnicity of the driver.

While these types of discrimination are often driven by the decisions of individual users of the platforms, they collectively create a discriminatory environment that can only be addressed through preventative interventions (MacKenzie, 2016). Finally, customer reviews can also be biased, which can unfairly limit employment prospects for workers (Berg 2016, p. 11).

5.2.3 Analysis and Opportunities

Digital labour platforms currently operate in a manner that is largely free of outside regulation, with power concentrated amongst a small number of global players. While this creates challenges for policymakers, stakeholders can work together to ensure labour protections and increase competition by modifying labour laws, changing business models and improving ToS.

Collective action

One of the overarching challenges presented by digital platforms is that their structure tends to create significant imbalances in power between platforms, clients and workers. Traditionally, when faced with asymmetries like this, workers have responded by organizing, and digital platform workers have, in several instances, begun to do so as well. This new form of organizing presents some opportunities for standards-based solutions.

The first opportunity for standards lies with digital platform co-operatives. These worker-led cooperative enterprises have recently begun to emerge as alternatives to centralized corporate-operated platforms. These platform co-ops are characterized by democratic governance and broad-based platform ownership. For example, many local cooperative platforms have emerged in the USA and EU to challenge ride-sourcing companies such as Uber and Lyft.[54] In Canada, Modo is one example of a local member-owned carshare service operating in British Columbia.[55]

While the emergence and success of these co-ops depend largely on the workers themselves, rule-setting organizations can play a role in enabling their success. SDOs already offer numerous standards which could help these co-ops achieve success and demonstrate their viability to governments and regulators. While many existing standards could be helpful, SDOs could make their standards more attractive by creating "packages" which might identify and include a number of standards drawn from different standards series that could be tailored to specific types of organizations, such as digital platform co-ops, based on their generic needs. These might include existing dispute resolution standards *(ISO 10003)* or data security standards *(ISO 27001),* for example. The creation of these packages, especially if done in cooperation with the co-ops themselves, might also help SDOs identify gaps that exist in their existing standards catalogue which they could then fill through the development of new standards or the modification of existing ones.

Another way in which social protections for digital workers can be increased is through collective bargaining. Based on the 1998 Declaration on Fundamental Principles and Rights at Work, the ILO's 187 member states have committed to ensuring "freedom of association and the effective recognition of the right to collective bargaining." This right is meant to be universal, without regard to employment status (Berg 2018, p. 105-106). A number of groups of digital platform workers, especially those who are geographically proximate, have already started to organize, such as the California App-Based Drivers Association.[56]

Should digital platform workers begin to unionize in greater numbers, SDOs can play an important role by convening discussions between platform and worker representatives to develop standards which could be referenced in collective agreements.[57] These might include standards on many of the issues discussed in this report, such as around access to, and portability of, work history and reputation data between platforms. In some cases, existing standards might be sufficient, but in other cases, new standards might be needed. For example, in response to the lack of a mechanism to rate clients on Amazon Mechanical Turk, two PhD students

[54] See https://platform.coop/about

[55] See: https://www.modo.coop/about/

[56] See, for example, Roberts (2018).

[57] One of the experts interviewed for this report stated that one of the scenarios most likely to produce good standards for heavily international economic sectors – that is, sectors where individual governments have difficulty regulating the workplace – is one where there is strong representation from both workers and employers.

developed a browser plug-in called Turkopticon to enable workers to review clients on aspects such as pay, speed of payment and fairness in evaluation (Berg et al. 2018, p. 79-81). Using this system as an inspiration, an SDO could develop a client review standard that could be included in future collective agreements between workers and platforms.

Platform responsibility

Alternatively, SDOs could develop a comprehensive digital labour platform standards framework analogous to the *ISO 26000* family of standards focused on social responsibility. In addition to standards, SDOs can also create a framework of best practices and guidance documents. Such an approach would involve developing standards for the entire range of platform operations not covered by already existing standards, and modifying existing standards to align them explicitly with digital labour platforms. Such a framework could focus on:

- **Fair compensation:** As discussed, low wages are a key contributor to the precarity experienced by many digital platform workers. To overcome this, a recent report from the ILO suggests that the minimum wage or living wage should be applied based on the worker's location to ensure fair compensation (Berg et al. 2018, p. 106-107). Additionally, such a standard could also include provisions such as any fees and payments deducted from a worker's wages should be transparently identified and explained in advance.
- **Benefits:** As they are deemed to be independent contractors or self-employed, digital platform workers do not receive the same benefits – such as sick days, extended health coverage or pensions – as standard workers. A benefits standard could provide a template for how platforms might structure a benefits framework whereby workers could, after putting in a certain number of hours worked or amount of work completed within a certain period of time, qualify for certain benefits (Choudary 2018, p. 37).[58]
- **Flexibility:** Given that flexibility is often regarded as a feature of platform work, workers should be able to exercise their freedom in the true sense by not being penalized for rejecting work or for not working a minimum number of hours (Berg et al. 2018, p. 106). A flexibility standard would set limits on the ways in which platforms would be allowed to direct or control the labour of workers.
- **Dispute resolution mechanisms:** A digital labour platforms dispute resolution standard could modify the existing dispute resolution standard by providing explicit guidance on how to resolve disputes common to these platforms, such as non-payment. This might include a requirement that clients provide justification for rejection and prohibition on clients' ability to use the work or own intellectual property for which they have not paid. It could also include a requirement that workers have a right to appeal to a neutral third party (Berg et al. 2018, p. 106-107).

6 Recommendations

As discussed in the preceding sections, there are many opportunities for standards-based solutions to contribute to the governance of the digital economy. This section provides four groups of recommendations through which SDOs can strategically seize these opportunities. These groups of recommendations have been assembled thematically, recognizing that many of the opportunities identified in preceding sections overlap or are complementary in character.

6.1. Investigate new technologies and approaches

Recommendation 1: Develop standards for digital ToS agreements

The GDPR and *California's Consumer Privacy Act* are two of the most advanced rule instruments for the digital economy, and both contain requirements that have implications for ToS agreements. The development of a standard for Canadian organizations that need to ensure that they are complying with the requirements contained in these two instruments, or simply wish to adopt best practices in this area, could be very useful. Canadian SDOs should consider developing such a standard which would include guidance on

[58] It may be difficult to apply this model to remote crowdwork platforms.

requirements such as meaningful consent, the right to opt out of unnecessary data collection, notification of data breaches and accessible language. Standards specifically focused on the governance needs of digital labour platforms, such as dispute resolution, could also be developed and could build on top of these more generic foundational standards.

Recommendation 2: Investigate the development of machine readable standards

The development of machine readable standards represents a critical step that needs to be taken for standards to play a larger role in the digital economy and especially in standards for software.[59] Moreover, the development of machine readable standards will be necessary for the introduction of greater efficiency and even automation into both the standards development process and the development of new approaches to the deployment and use by consumers of standards, such as the digital registry of accreditations suggested below.

Recommendation 3: Investigate the development of a digital registry of standards accreditations

For consumer-facing standards and, increasingly, for enterprise-facing standards or standards that play a role in supply chains or insurance policies to be effective – it must be possible to quickly, easily and reliably recognize when a product or service has been certified.[60] This likely means that greater automation needs to be introduced into this process. This can be difficult for software-based products and services that rely on non-digital certifications. Graphical kitemarks can be easily copied in the digital space and, given the rate at which software is updated, genuine adherence to a standard can quickly erode over time. The emergence of blockchain and distributed ledger technology, however, potentially offers a technological solution to this problem. A digital registry could provide the reliable, easily updatable digital record of certifications needed to increase the usefulness of standards in the digital economy. It could serve as the basis for a number of tools, such as web browser plug-ins, that would enable users to quickly and easily check which standards an app, service, platform or website adheres to. When combined with machine readable standards, digital registries could enable the automation that these processes require.

Recommendation 4: Begin developing standards for a decentralized web

The digital economy is currently dominated by a small number of powerful firms, a situation which this report has argued is producing a number of harmful effects. This assessment is not unique and many technologists are actively working on developing tools that will enable a more decentralized Internet in the future. These range from those focused on blockchain, to the Solid project, to others like the InterPlanetary File System (IPFS).[61] Standards will be critical to ensuring interoperability in the decentralized web, because a decentralized web will lack dominant firms capable of imposing/providing their own standards. Hence, SDOs have an opportunity to make an important contribution. Critically, however, SDOs will need to figure out how to better interact with the open source approach to software development.

Recommendation 5: Consider developing algorithmic predatory pricing and tacit collusion "incubators"

Algorithms that engage in predatory pricing and tacit collusion represent an important potential economic challenge. While many organizations will likely consider developing tools for identifying cases of algorithms engaging in problematic behaviour, SDOs and certification bodies may find that the ability to identify and certify algorithms that will not engage in these behaviours represents an important service. Developing such incubators will be difficult, however, and doing so will require SDOs to begin soon and conduct this work collaboratively with legal, economic and computer science experts.

Recommendation 6: Develop "standards packages"

While primarily a marketing approach, this recommendation is aimed at making standards more accessible to organizations that are less familiar with standards-based approaches. As demonstrated by some of this report's findings, such as a lack of consumer

[59] A standards expert made this point during a research interview conducted for this report.

[60] This claim was made by a standards expert interviewed for this report.

[61] For more information see https://ipfs.io/

experience with standards in digital contexts and the limited take-up of existing cybersecurity standards, it is clear that even existing standards are not being used to their full potential in the digital context. By providing off the shelf lists of standards tailored to the needs of specific types of organizations (digital transportation platform; healthcare start-up; medium-sized municipal government), SDOs could increase the uptake of standards by organizations without deep knowledge of standards. The act of assembling these lists could also help to identify gaps in the existing standards catalogue, thereby providing direction for future work.

6.2. New standards for data and AI

Recommendation 7: Develop standards for industrial data and industrial AI implementations

One of this report's clearest findings is that there are significant opportunities for data standardization to positively impact Canadian industry. Canadian industrial firms could become more efficient and productive if they were able to increase the interoperability of their systems and develop more sophisticated algorithms to improve their supply chains. In addition to calls for more help in this regard from government, there is a clear openness to working with SDOs to develop industry-specific data standards that would enable greater compatibility between industrial systems and to begin leveraging industrial data for training AIs. SDOs should work with these organizations, the AI supply chain supercluster and relevant government departments and agencies like Statistics Canada to develop the standards they need (Hirsh, 2019).

Recommendation 8: Incorporate the "lawnmower of justice" concept into standards for AI training data

AI has already begun to digitally reproduce and reinforce the biases and patterns of discrimination that exist in society. Ensuring that AI represents a step forward for humanity will require making sure that it does not become irretrievably tainted by the discrimination encoded in the data used to train it. The "lawnmower of justice" approach is an exciting attempt to overcome this problem. SDOs should seek to integrate this and other similar concepts into data standards and standards developed for the training of AI.

Recommendation 9: Develop standards for the use of AI decision-making systems by governments and public institutions

A 2018 report examined the Government of Canada's use of an AI decision-making system in its immigration application process (Molnar and Gill, 2018). This report highlighted a number of concerns around the use of AI in contexts where public organizations were making decisions that impact individuals in significant ways. The report also offered an in-depth description of the steps that governments ought to take in order to use AI in ethical ways. SDOs should consider developing standards for the use of AI decision-making systems by governments and public institutions. This could include implementing some of the recommendations advanced in this report.

Recommendation 10: Develop standards that enable downstream user control of their data

As legal and regulatory constraints increase, using user data for analytics and training AI will become increasingly difficult for organizations. While this shift will be largely positive, it will also introduce new obstacles to the use of this data for beneficial purposes. Already, significant pools of data collected by the public sector, which could produce significant benefits, are not being used fully because of privacy concerns. The development of "smart data" standards that would enable users to set controls on how their data is used which would persist as that data flows through value chains could help to balance the protection of privacy with beneficial uses of data.[62]

6.3. Legal and regulatory compliance

Recommendation 11: Canadian SDOs should respond to any updating of Canada's privacy regime by creating complementary standards

Numerous organizations have begun using ISO standards to show due diligence in their fulfillment of the new privacy requirements created by the GDPR. Should the Government of Canada update its privacy regime, Canadian SDOs should prepare a "package" of standards which they can make available to organizations so they can do the same for any new Canadian privacy requirements. In the process

[62] One model for how this could be done would be to examine Creative Commons licences https://creativecommons.org/licenses/

of curating such a package, Canadians SDOs could also identify any international standards that require modifications for the Canadian context and any gaps in the existing standards catalogue. Should such gaps be identified, Canadians SDOs ought to take steps to fill them.

6.4 Digital platform standards

Recommendation 12: Develop data standards to enable portability of personal data between platforms

Increasing competition between digital platforms will be critical to spurring the creation of alternative digital business models, like those that could underpin a decentralized web. Combined with the development of "smart data" standards recommended earlier, the development of standards designed to make user data portable between platforms would significantly encourage competition. More and more jurisdictions now require that platforms provide users with this data – which can take many forms ranging from purchase histories from digital marketplaces; to posts, social connections and interactions from social media platforms; to work history data from digital labour platforms – to users upon request. The creation of data portability standards could enable users to begin transferring this data between platforms, an ability that could radically transform the digital economy.

Recommendation 13: Consider developing standards on digital platform labour rights

Because of their transnational reach, digital labour platforms are unlikely to be the subjects of effective national regulation or legislation in the near future. This presents an opportunity for a standards-based approach to make significant contributions in this area. As was the case with the development of the ISO 26000 series of social responsibility standards, framework standards on digital platform labour responsibilities would include requirements around issues such as payment of wages, protection for workers' intellectual property, clear rules around how to determine minimum wages and equitable dispute resolution systems. In addition to standards, SDOs can also develop best practice and guidance documents for digital platform stakeholders.

7 Conclusion

It can be easy to forget how new the digital economy is. The World Wide Web was only invented 30 years ago. User-friendly web browsers are only 25 years old. Mobile computing, today's dominant computing paradigm, only really took off with the launch of the iPhone, a paltry 12 years ago.

The novelty of the digital economy is an important factor in the limited nature of its governance regime. But there are also other major factors at play. The transnational character of the Internet; the technical, and thus often opaque, nature of its underpinnings; the vested interests of a number of extremely powerful and popular firms; and the often obscured preference on the part of powerful governments to keep the Internet relatively ungoverned so as to enable offensive military and intelligence operations, have all contributed to the current situation.

Nonetheless, not only are there significant opportunities for standards-based solutions to play a role in improving this situation, in many instances, standards may offer the best available means of doing so due to SDOs' credibility, international connections and ability to bring together expertise from diverse domains. This report highlighted three such areas, namely: data governance, algorithms and AI, and digital platforms. In each of these areas, standards can play a vital role in safeguarding public interest and promoting ethics, as well as increasing competition and levelling the playing field.

Nonetheless, designing new governance instruments – standards-based or otherwise – will not be easy. Powerful vested interests and obstacles inherent to the digital realm are sure to push against progress. But this reality is merely a reminder of the need to be proactive, smart and strategic; as well as the critical importance of diverse stakeholders from the civil society coming together to develop solutions.

The opportunities for standards-based solutions to make a positive contribution to the governance of the digital economy are numerous and significant. SDOs must not hesitate to seize them.

References

Alwani, K. and Urban, M.C. (February 2019). Maximizing the Gains From Sharing: An Analysis of National and International Best Practices. *CSA Group.* Retrieved from https://www.csagroup.org/article/maximizing-the-gains-from-sharing-an-analysis-of-national-and-international-best-practices/

Angwin, J. Larson, J. Mattu, S. Kirchner, L. ProPublica. (23 May, 2016). Machine Bias. *ProPublica.* Retrieved from https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Baynes, C. (2 May, 2018). Government 'deported 7,000 foreign students after falsely accusing them of cheating in English language tests.' *The Independent.* Retrieved from https://www.independent.co.uk/news/uk/politics/home-office-mistakenly-deported-thousands-foreign-students-cheating-language-tests-theresa-may-a8331906.html

BBC News. (24 December, 2014). Uber 'truly sorry' for price rise during Sydney siege. *BBC News.* Retrieved from https://www.bbc.com/news/technology-30595406

BBC News. (27 January, 2016). Google achieves AI 'breakthrough' by beating Go champion. *BBC News.* Retrieved from https://www.bbc.com/news/technology-35420579

BBC News. (17 February, 2017). German parents told to destroy Cayla dolls over hacking fears. *BBC News*. Retrieved from https://www.bbc.com/news/world-europe-39002142

Berg, J. (2016). Income security in the on-demand economy: Findings and policy lessons from a survey of crowdworkers. *International Labour Organization.* Retrieved from https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

Berg, J. Furrer, M. Harmon, E. Rani, U. Silberman, M.S. (2018). Digital labour platforms and the future of work: Towards decent work in the online world. *International Labour Organization.* Retrieved from https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_645337.pdf

Block, S. and Hennessy, T. (April 2017). "Sharing economy" or on-demand service economy? A survey of workers and consumers in the Greater Toronto Area. *Canadian Centre for Policy Alternatives | Ontario.* Retrieved from https://www.policyalternatives.ca/sites/default/files/uploads/publications/Ontario%20Office/2017/04/CCPA-ON%20sharing%20economy%20in%20the%20GTA.pdf

Brogan, J. (2 February, 2016). What's the Deal With Algorithms? *Slate.* Retrieved from http://www.slate.com/articles/technology/future_tense/2016/02/what_is_an_algorithm_an_explainer.html

Canada's Economic Strategy Tables. (No date). *Digital Industries: The sector today and opportunities for tomorrow | Interim Report.* Retrieved from https://www.ic.gc.ca/eic/site/098.nsf/vwapj/ISEDC_Table_DI.pdf/$file/ISEDC_Table_DI.pdf

Cassar, C. Heath, D. Micallef, L. (No date). *What is digital economy?* Unicorns, transformation and the internet of things. Retrieved from https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html

CBC Radio. (9 September, 2018). Why computer science students are demanding more ethics classes. *Spark.* Retrieved from https://www.cbc.ca/radio/spark/spark-404-1.4811760/why-computer-science-students-are-demanding-more-ethics-classes-1.4812742

Chan, D. (20 October, 2017). The AI That Has Nothing to Learn From Humans. *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2017/10/alphago-zero-the-ai-that-taught-itself-go/543450/

Choudary, S. P. (2018). The architecture of digital labour platforms: Policy recommendations on platform design for worker well-being. *International Labour Organization.* Retrieved from https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_630603.pdf

Coglianese, C. Lehr, D. (Forthcoming). Transparency and Algorithmic Governance. *Administrative Law Review/ University of Pennsylvania Law School, Public Law Research Paper* No. 18-38. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3293008

Constine, J. (21 February, 2019). Facebook pays teens to install VPN that spies on them. *TechCrunch.* Retrieved from https://techcrunch.com/2019/01/29/facebook-project-atlas/

Deane, H. (2017). Dynamic Pricing – Can consumers achieve the benefits they expect? *Consumers Council of Canada.* Retrieved from https://www.consumerscouncil.com/dynamic-pricing-download

Ditta, S. Thirgood, J. Urban, M.C. (14 May, 2017). *The Rise of the Sharing Economy: Exploring standards-based solutions in a changing marketplace.* Retrieved from https://www.csagroup.org/article/rise-of-the-sharing-economy/

The Economist. (8 April, 2017a). How to manage the computer-security threat. *The Economist.* Retrieved from https://www.economist.com/leaders/2017/04/08/how-to-manage-the-computer-security-threat

The Economist. (8 April, 2017b). Computer security is broken from top to bottom. *The Economist.* Retrieved from https://www.economist.com/science-and-technology/2017/04/08/computer-security-is-broken-from-top-to-bottom

The Economist. (6 May, 2017). The world's most valuable resource is no longer oil, but data. The Economist. Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The Economist. (2 June, 2018). American tech giants are making life tough for startups. *The Economist.* Retrieved from https://www.economist.com/business/2018/06/02/american-tech-giants-are-making-life-tough-for-startups

The Economist. (23 August, 2018). The business of insuring intangible risks is still in its infancy. *The Economist.* Retrieved from https://www.economist.com/finance-and-economics/2018/08/23/the-business-of-insuring-intangible-risks-is-still-in-its-infancy

The Economist. (2 October, 2018). Babbage: The Nobel winners explained. *The Economist.* Retrieved from https://soundcloud.com/theeconomist/babbage-the-nobel-winners

The Economist. (20 March, 2019). Uber drivers demand their data. *The Economist.* Retrieved from https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data

Ensign, D. Friedler, S. A. Neville, S. Scheidegger, C. Venkatasubramanian, S. (2018). Runaway Feedback Loops in Predictive Policing. *Proceedings of Machine Learning Research,* 81. 1–12. Retrieved from https://arxiv.org/abs/1706.09847

EU GDPR.org (No date). *GDPR Key Changes.* Retrieved from https://eugdpr.org/

Ezrachi, A. and Stucke, M. E. (2016). *Virtual Competition: The Promise and Perils of the Algorithm-driven Economy.* Cambridge, Massachusetts: Harvard University Press.

Feldman, B. (30 January, 2019). Apple Disables Facebook Apps Following News of Shady Research Project. *Intelligencer.* Retrieved from http://nymag.com/intelligencer/2019/01/apple-disables-facebook-apps-used-for-invasive-research.html

Field, F. and Forsey, A. (September 2016). Wild West Workplace: Self-employment in Britain's 'gig economy.' Retrieved from http://www.frankfield.co.uk/upload/docs/Wild%20West%20Workplace.pdf

Fleming, N. 30 May, 2018. How artificial intelligence is changing drug discovery. *Nature: International Journal of Science*, 557, S55-S57. doi: 10.1038/d41586-018-05267-x.

Fraser, K. (30 August, 2018). Duncan man files class-action lawsuit after cyber attack at Equifax. *Vancouver Sun.* Retrieved from https://vancouversun.com/news/local-news/duncan-man-files-class-action-lawsuit-after-cyber-attack-at-equifax

Friedersdorf, C. (12 May, 2018). YouTube Extremism and the Long Tail. *The Atlantic.* Retrieved from https://www.theatlantic.com/politics/archive/2018/03/youtube-extremism-and-the-long-tail/555350/

Ghebreslassie, M. Taylor, C. Singh, A. (16 November, 2018). Ontario workplace safety board reviewing Uber Eats following Marketplace investigation. *CBC News.* Retrieved from https://www.cbc.ca/news/canada/marketplace-food-delivery-apps-labour-issues-1.4895801

Girard, M. (16 January, 2019). *Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter.* Retrieved from https://www.cigionline.org/publications/big-data-analytics-need-standards-thrive-what-standards-are-and-why-they-matter

Graham, M. Hjorth, I. Lehdonvirta, V. (2017). Digital labour and development: impacts of global digital labour platforms and the gig economy on worker livelihoods. *Transfer: European Review of Labour and Research, 23*(2). 135-162.

Greenberg, A. (21 July, 2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired.* Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greenberg, A. (9 February, 2018). An AI That Reads Privacy Policies So That You Don't Have To. Wired. Retrieved from https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/

A Guide to the Internet of Things: How Billions of Online Objects Are Making the Web Wiser. (No date). Retrieved from https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png

Hirsh, J. (4 February, 2019). A Case for Reimagining Canadian Data Standards. Retrieved from https://www.cigionline.org/articles/case-reimagining-canadian-data-standards

Ince, J. (29 March, 2017). How to Fix Uber and Lyft's Rating System. *The Rideshare Guy.* Retrieved from https://therideshareguy.com/how-to-fix-uber-and-lyfts-rating-system/

Information and Privacy Commissioner of Ontario. (July 2014a) *Ontario's Freedom of Information and Protection of Privacy Act: A Mini Guide.* Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/provincial%20guide-e.pdf

Information and Privacy Commissioner of Ontario. (July 2014b). *Ontario's Municipal Freedom of Information and Protection of Privacy Act: A Mini Guide.* Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/municipal%20guide-e.pdf

Information and Privacy Commissioner of Ontario. (August 2014). *Your Privacy & Ontario's Information and Privacy Commissioner.* Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/Your_Privacy-e.pdf

Joyce, S. Holcomb, C. Cline, J. Aqua, J. (No date). 10 considerations to help position the GDPR data protection officer for success. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/general-data-protection-regulation/data-protection-officer-10-considerations.html

Khan, L. M. (2017). Amazon's Antitrust Paradox. *The Yale Law Journal,* 126(3). 710-805. Retrieved from https://www.yalelawjournal.org/note/amazons-antitrust-paradox

Lant, K. (21 July, 2017). Experts Want Robots to Have an "Ethical Black Box" That Explains Their Decision-Making. *Futurism.* Retrieved from https://futurism.com/experts-want-robots-to-have-an-ethical-black-box-that-explains-their-decision-making/

Lapowsky, I. 28 June, 2018. California Unanimously Passes Historic Privacy Bill. *Wired.* Retrieved from https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/

Larson, S. (4 October, 2017). Every single Yahoo account was hacked - 3 billion in all. *CNN Business.* Retrieved from https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

Lewis, P. (6 October, 2017).'Our minds can be hijacked': the tech insiders who fear a smartphone dystopia. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia

MacKenzie, D. (31 October, 2016). Do ride-sourcing drivers discriminate against passengers? Sustainable *Transportation Lab.* Retrieved from https://faculty.washington.edu/dwhm/2016/10/31/do-ride-sourcing-drivers-discriminate-against-passengers/

Marr, B. (21 May, 2018). How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. *Forbes.* Retrieved from https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#7a42727360ba

McDonald, B. (2 February, 2018). Canada not ready for driverless cars, Senate report says. *Quirks and Quarks.* Retrieved from https://www.cbc.ca/radio/quirks/canada-not-ready-for-driverless-cars-senate-report-says-1.4517064

Meyer, R. (8 March, 2018). The Grim Conclusions of the Largest-Ever Study of Fake News. *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/

Molnar, P. Gill, L. (2018). Bots and the Gate: A Human Rights Analysis of Automated Decision-making in Canada's Immigration and Refugee System. *International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto).* Retrieved from https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf

Murphy Jr, B. (13 March, 2018) People Are Suing Equifax in Small-Claims Court and It's Totally Brilliant. Here's Why. *Inc.* Retrieved from https://www.inc.com/bill-murphy-jr/people-are-suing-equifax-in-small-claims-court-its-totally-brilliant-heres-why.html

Ng, A. (7 September, 2018). How the Equifax hack happened, and what still needs to be done. *c|net.* Retrieved from https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/

Noack, A. and Vosko, L. (November 2011). Precarious Jobs in Ontario: Mapping Dimensions of Labour Market Insecurity by Workers' Social Location and Context. *Law Commission of Ontario.* Retrieved from https://www.lco-cdo.org/wp-content/uploads/2012/01/vulnerable-workers-call-for-papers-noack-vosko.pdf

O'Neil, C. (2017). Weapons of Math Destruction: *How Big Data Increases Inequality and Threatens Democracy.* New York: Broadway Books. Introduction.

Office of the Privacy Commissioner of Canada. (31 January, 2018). *Summary of privacy laws in Canada.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Office of the Privacy Commissioner of Canada. (9 January, 2018). *PIPEDA in brief.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Office of the Privacy Commissioner of Canada. (23 November, 2018). National Digital and Data Consultations: Submission to Innovation, Science and Economic Development Canada. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ised_181123/

Office of the Privacy Commissioner of Canada. (14 December, 2018). *The Privacy Act.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/

Office of the Privacy Commissioner of Canada. (5 February, 2019). *The Personal Information Protection and Electronic Documents Act (PIPEDA).* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Popper, B. (8 July, 2014). Uber agrees to new national policy that will limit surge pricing during emergencies. **The Verge.** Retrieved from https://www.theverge.com/2014/7/8/5881535/uber-price-gouging-surge-pricing-new-york-agreement

Powles, J. (20 December, 2017). New York City's Bold, Flawed Attempt to Make Algorithms Accountable. *The New Yorker.* Retrieved from https://www.newyorker.com/tech/annals-of-technology/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

Rieland, R. (5 March, 2018). Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased? *Smithsonian.com.* Retrieved from https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/

Rizza, A. (9 December, 2018). Critics call for more transparency on high-tech Sidewalks Lab project in Toronto. *The Globe and Mail.* Retrieved from https://www.theglobeandmail.com/business/technology/article-critics-call-for-more-transparency-on-high-tech-sidewalks-lab-project/

Roberts, Y. (1 July, 2018). The tiny union beating the gig economy giants. *The Guardian.* Retrieved from https://www.theguardian.com/politics/2018/jul/01/union-beating-gig-economy-giants-iwgb-zero-hours-workers

Roettgers, J. (29 June, 2018). California's New Privacy Law Could Have Big Impact on Tech, Media. *Variety.* Retrieved from https://variety.com/2018/digital/news/california-ab-375-1202861680/

Ronstedt, M. Eggert, A. (4 July, 2018). Among Blockchain-Friendly Jurisdictions, Malta Stands Out. *Coindesk.* Retrieved from https://www.coindesk.com/among-blockchain-friendly-jurisdictions-malta-stands-out

Rose-Stockwell, T. (30 April, 2018). Facebook's problems can be solved with design. *Quartz.* Retrieved from https://qz.com/1264547/facebooks-problems-can-be-solved-with-design/

Safian, R. (11 September, 2018). 5 lessons of the AI imperative, from Netflix to Spotify. *Fast Company.* Retrieved from https://www.fastcompany.com/90234726/5-lessons-of-the-ai-imperative-from-netflix-to-spotify

Scassa, T. (16 May, 2018) Considerations for Canada's National Data Strategy. In Medhora, R. (ed.), *Data Governance in the Digital Age.* (pp. 6-11). Retrieved from https://www.cigionline.org/publications/data-governance-digital-age

Scassa, T. (29 January, 2019). *Is Canada Ready for Open Banking?* Retrieved from https://www.cigionline.org/articles/canada-ready-open-banking

Schneier, B. (9 February, 2017). Security and Privacy Guidelines for the Internet of Things. *Schneier on Security.* Retrieved from https://www.schneier.com/blog/archives/2017/02/security_and_pr.html

Schneier, B. (2018). *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World.* New York: W. W. Norton & Company.

Schmidt, F. A. (2017). Digital Labour Markets in the Platform Economy: Mapping the Political Challenges of Crowd Work and Gig Work. Retrieved from https://library.fes.de/pdf-files/wiso/13164.pdf

Seals, T. (19 November, 2018). Ford Eyes Use of Customers' Personal Data to Boost Profits. *Threat Post.* Retrieved from https://threatpost.com/ford-eyes-use-of-customers-personal-data-to-boost-profits/139209/

Smith, A. (5 September, 2018). Many Facebook users don't understand how the site's news feed works. *Pew Research Centre.* Retrieved from https://www.pewresearch.org/fact-tank/2018/09/05/many-facebook-users-dont-understand-how-the-sites-news-feed-works/

Standards Council of Canada. (No date). Chapter 1 – What are standards? Retrieved from https://www.scc.ca/en/stakeholder-participation/orientation-modules/intro-to-standards-and-scc/chapter-1-what-are-standards

Statisa. (2019a). Retail e-commerce sales worldwide from 2014 to 2021 (in billion U.S. dollars). *Statisa.* Retrieved from https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Statisa. (2019b). E-commerce as percentage of total retail sales in Canada from 2013 to 2020. *Statisa.* Retrieved from https://www.statista.com/statistics/379117/e-commerce-share-of-retail-sales-in-canada/

Statistics Canada. (28 February, 2017). The sharing economy in Canada. *The Daily.* Retrieved from https://www.statcan.gc.ca/dailyquotidien/170228/dq170228b-eng.htm

Statistics Canada. (29 August, 2018). Digital economy, July 2017 to June 2018. *The Daily.* Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/180829/dq180829b-eng.htm

Stinson, C. (6 December, 2018). *I read the Terms of Service, so that you don't have to.* Retrieved from https://mowatcentre.ca/i-read-the-terms-of-service-so-that-you-dont-have-to/

Stucke, M.E. Ezrachi, A. (2017). Two Artificial Neural Networks Meet in an Online Hub and Change the Future (Of Competition, Market Dynamics and Society). *Oxford Legal Studies/ University of Tennessee*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2949434

Thomas, H. Kimber, A. Brown, W. (6 March, 2019). How regulation is unlocking the potential of open banking in the UK. *EY.* Retrieved from https://www.ey.com/en_gl/banking-capital-markets/how-regulation-is-unlocking-the-potential-of-open-banking-in-the-uk

Treviranus, J. (30 October, 2018). Sidewalk Toronto and Why Smarter is Not Better*. Retrieved from https://medium.com/datadriveninvestor/sidewalk-toronto-and-why-smarter-is-not-better-b233058d01c8

Valinsky, J. (30 November, 2018). Marriott reveals data breach of 500 million Starwood guests. *CNN Business.* Retrieved from https://www.cnn.com/2018/11/30/tech/marriott-hotels-hacked/index.html

Vallance, C. (29 February, 2016). Ukraine cyber-attacks 'could happen to UK'. *BBC News.* Retrieved from https://www.bbc.com/news/technology-35686493

Wachter, S. Mittelstadt, B. Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

Weinberger, D. (28 Janaury, 2018). Optimization over Explanation. *Berkman Klein Centre.* https://medium.com/berkman-klein-center/optimization-over-explanation-41ecb135763d

What We Heard: Modernizing Federal Labour Standards. (30 August, 2018). *Employment and Social Development Canada.* Retrieved from https://www.canada.ca/content/dam/canada/employment-social-development/campaigns/labour-standards/1548-MLS_WWH-Report_EN.pdf

Whittaker, Z. (10 December, 2018). Equifax breach was 'entirely preventable' had it used basic security measures, says House report. *TechCrunch.* Retrieved from https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/

Youyou, W. Kosinski, M. Stillwell. D. (January 2015). Computers judge personalities better than humans. *Proceedings of the National Academy of Sciences,* 112 (4). 1036-1040.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology,* 30, 75–89. doi:10.1057/jit.2015.5

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™