Policy Overview

Research and Policy Making Through the Data of Platform Enterprises

Katherine Reilly
Carol Muñoz Nieves

IT for Change | March 2020

This report was produced as part of the research project ‘Policy frameworks for digital platforms - Moving from openness to inclusion’. The project seeks to explore and articulate institutional-legal arrangements that are adequate to a future economy that best serves the ideas of development justice. This initiative is led by IT for Change, India, and supported by the International Development Research Centre (IDRC), Canada.

Authors

Katherine Reilly is Associate Professor in the School of Communications at Simon Fraser University in Vancouver, Canada.

Carol Muñoz Nieves is a Cuban scholar in the field of mass communication and media industries.

Research coordination team

Principal Investigator: Anita Gurumurthy
Co-investigators: Deepti Bharthur, Nandini Chami
Editorial Support: Shruti Sunderraman, Deepti Bharthur
Design: Purnima Singh

© IT for Change 2020

Licensed under a Creative Commons License Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4)

IT for Change

IDRC | CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

Data and the Platform Economy in Canada: A Policy State-Of-Play Report

Policy Overview

March 2020

Katherine Reilly

Carol Muñoz Nieves

Page intentionally left blank

1. Introduction

At the federal level, Canada is entering a new policy cycle where data and digital industries are concerned. A number of factors are contributing to this situation. After a decade of conservative leadership, the Liberals came to power in 2015 under the current prime minister, Justin Trudeau. One of Trudeau's campaign platforms was a promise to review the innovation policy and develop a new Innovation Agenda for Canada.[1] At the same time, significant changes in foreign data policies such as the new General Data Protection Regulation (GDPR) of the European Union (EU), as well as ongoing trade negotiations including the Comprehensive Economic Trade Agreement (CETA) with the EU, the Trans-Pacific Partnership (TPP), and the revision of the North American Free Trade Agreement (NAFTA), are also putting pressure on Canada to reconsider its data policies. Finally, Canada's existing data-policy framework is increasingly seen as exhausted, leading to demands for a general overhaul of the country's approach to regulating private sector data.

All together, these forces are generating calls for the development of a new National Data Policy for Canada, however no clear mandate has arisen yet to pursue this goal. This paper explores these factors in greater detail, explaining how they are relevant to the platform economy in Canada. It then discusses Canada's current data policies, and the surrounding policy community, which is currently in transition. Finally, it lays out some of the limitations of the current data-policy framework in Canada, and suggests ways in which the platform economy may influence a discussion around policy reform or renovation.

2. Factors Driving Demand for Data Policy Reform

In Trudeau's 2015 campaign platform, he promised to invest in a new Innovation Agenda for Canada with a particular focus on schemes to incubate business innovation and accelerate time-to-market for new innovations.[2] The Agenda also promised to provide support for strategic innovation clusters across the country. While innovation is not a new agenda for the Canadian government, the Liberals are revisiting it with new vigor. Research and development by Canadian firms dropped off during the Harper years (2006-2015) (data.oecd.org), as the country turned to the resource sector as its primary motor of growth. The thinking under Trudeau shifted to the idea that Canada should invest in innovation to strengthen other sectors of the economy in the face of both climate change and growing global competition to the country's resource-based economy.

In 2016, Canada ranked 14th on the Networked Readiness Index (NRI), prepared by the World Economic Forum, having "improve[d] its absolute performance but less than its peers, thus sliding down three positions[3]" in comparison to 2014. The NRI assesses the factors, policies, and institutions that enable a country to fully leverage information and communication technologies (ICTs) for increased competitiveness and well-being. According to the performance review presented in this report,

> "The country [Canada] can rely on one of the best business and innovation environments in the world (4th), where starting a business is easy and quick (ranking 3rd on both time and procedures to start a business). The potential of a highly skilled workforce (11th) remains partially untapped, as individual usage remains relatively low (30th): for example, there are only 54.3 mobile broadband subscriptions per 100 people in Canada (52nd), compared to 102.7 in the United States. Although the government has been quite successful in using digital technologies to provide online services (10th) and allow citizens' e-participation (14th), it has not shown a strong vision for ICTs (49th) nor has it been particularly successful in promoting them (38th). This might change in the future

1 https://trudeaumetre.polimeter.org/promise/2309
2 Ibid.
3 http://reports.weforum.org/global-information-technology-report-2016/economies/#economy=CAN

> because the government is stepping up efforts to promote innovation policies, which will need to include a strong ICT component. Once an innovation leader in the mobile industry, Canada still relies heavily on mining and medium-technology sectors. Improving businesses' adoption of ICTs (22nd) can be a powerful driver of innovation for the country." (p.27)

The Liberals' first federal budget in 2016 pledged "to build Canada as a centre of global innovation" making innovation a central plank of their governance agenda. To begin with, the government established a series of Economic Strategy Tables to consult with industry leaders. This included a Digital Industries Table chaired by Tobias Lütke, Founder and CEO of Shopify, Canada's flagship platform enterprise. The 2017 budget went on to announce a competition to identify business-led innovation superclusters. On February 15, 2018, Navdeep Bains, Minister of Innovation, Science and Economic Development, announced five winners of this competition, one of which includes a digital technology supercluster to be based in British Columbia.[4] Its goal is to use "big data and digital technologies to unlock new potential in important sectors like healthcare, forestry, and manufacturing." The project describes its work in this way:

> "If the prize resource of the 20th century was oil, the prize resource of the 21st century is data. Canada will be a global leader through a digital technology supercluster that unlocks the potential of data for the intelligent enterprise. Starting from the West Coast and engaging with companies from across Canada, our supercluster will make the digital future a competitive advantage for Canada's industries."[5]

The framing of this innovation cluster is interesting. In 2016, Canada's tech sector accounted for 7.1 percent of the country's economic output (about $105 billion), 6.1 percent of Canadian firms, and 5.6 percent of total employment. And yet, at over $9.1 billion per year, it was by far Canada's largest investor in R&D.[6] It is notable, then, that the digital technology cluster will focus on helping traditional industries incorporate digital innovations, including those related to Big Data into their work. As we shall see, this is sure to include leveraging business practices pioneered within the platform economy, and translating them into other areas of the economy.
It is also worth noting that the 2017 budget also provided support for a review of Canadian intellectual property (IP) policy, with the goal of ensuring that, "Canada's IP regime is modern and is intended to support commercializing Canadian innovation and creativity, foster an ecosystem that supports businesses to grow to scale,

4 In 2017, the federal government announced a competition, looking for proposals from industry-led groups for the sponsorship of innovation programs (Innovation, Science and Economic Development Canada, 2018a). After two rounds of elimination, five clusters were announced in early 2018, up to $950 billion of total investment: 1) Digital Technology Supercluster. Regional concentration: British Columbia. Technology focus: Virtual, mixed and augmented reality; data collection and analytics; quantum computing (2018b); 2) Protein Industries Supercluster. Regional concentration: Prairie Provinces. Technology focus: Agri-food enabling technologies, including genomics, processing, and information technology (IT) (Innovation, Science and Economic Development Canada, 2018c); 3) Advanced Manufacturing Supercluster. Regional concentration: Ontario. Technology focus: Internet of Things, machine learning, cybersecurity, additive manufacturing (3D printing) (Innovation, Science and Economic Development Canada, 2018d); 4) AI-Powered Supply Chains Supercluster (SCALE.AI). Regional concentration: Based in Quebec and spanning the Quebec-Windsor corridor. Technology focus: Artificial intelligence and supply chain technology (Innovation, Science and Economic Development Canada, 2018e); 5) Ocean Supercluster. Regional concentration: Atlantic Canada: Technology focus: Digital sensors and monitoring, autonomous marine vehicles, energy generation, automation, marine biotechnology and marine engineering technologies (Innovation, Science and Economic Development Canada, 2018f).
Innovation, Science and Economic Development Canada (2018a, February 15) "Government of Canada's new innovation program expected to create tens of thousands of middle-class jobs." https://www.canada.ca/en/innovation-science-economic-development/news/2018/02/government_of_canadasnewinnovationprogramexpectedtocreatetensoft.html
Innovation, Science and Economic Development Canada (2018b) Digital Technology Supercluster. https://www.ic.gc.ca/eic/site/093.nsf/eng/00011.html
Innovation, Science and Economic Development Canada (2018c) Protein Industries Supercluster. https://www.ic.gc.ca/eic/site/093.nsf/eng/00012.html
Innovation, Science and Economic Development Canada (2018d) Advanced Manufacturing Supercluster. https://www.ic.gc.ca/eic/site/093.nsf/eng/00010.html
Innovation, Science and Economic Development Canada (2018e) AI-Powered Supply Chains Supercluster (SCALE.AI). https://www.ic.gc.ca/eic/site/093.nsf/eng/00009.html
Innovation, Science and Economic Development Canada (2018f) Ocean Supercluster https://www.ic.gc.ca/eic/site/093.nsf/eng/00013.html
5 https://www.digitalsupercluster.ca/wp-content/uploads/2018/01/Canadas-Digital-Technology-Supercluster-Executive-Summary.pdf
6 http://brookfieldinstitute.ca/research-analysis/the-state-of-canadas-tech-sector-2016/

and ensure that firms have the awareness and incentive to strategically use IP to grow and compete."[7] In other words, the IP regime needs to focus on bringing Canadian innovation to market.

Experts at StatsCan argue that it is incorrect to think of sharing as a sector. It is more correct to think of it as a business practice which, like innovation itself, should be measured across business sectors

---

This scenario helps us put Canada's sharing economy into perspective. When measured as a 'sector,' the sharing economy forms a small part of the discussion about digital innovation in Canada. While we still lack strong figures about the size of the sharing economy, a 2017 study by Statistics Canada found that between November 2015 and October 2016, Canadians spent approximately CD$1.3 billion on peer-to-peer ride sharing services and private accommodation services combined (both domestically and while abroad, using both domestic and foreign service providers).[8] This figure accounts for only 0.06 percent of the national GDP -- but Canada can't even claim all of this wealth because some service providers are located in other jurisdictions. To offer further perspective, Canadian networked media industries (a compendium of telecom, media and internet companies) were worth $77 billion in 2015, accounting for almost 4 percent of the GDP. The 10 largest media companies in Canada are, in order: Bell, Rogers, Telus, Shaw (Corus), Quebecor (Videotron), Google, CBC, Facebook, Sasktel, and Postmedia. The "big 5" Canadian companies' revenues are many times higher than the Canadian revenues of US internet giants.[9]

However, Statistics Canada points out that their figures may underestimate the contributions of sharing activities to the economy, given the complexity of capturing the different types of services provided and consumed by both domestic and international operators in sharing economy operations.[10] (Indeed, Statistics Canada produced the figures cited above as part of a learning exercise. They are part of an OECD working group that is developing new strategies for measuring sharing practices.) Furthermore, experts at StatsCan argue that it is incorrect to think of sharing as a sector. It is more correct to think of it as a business practice which, like innovation itself, should be measured across business sectors. This is, of course, much more difficult to do, and we do not currently have any way of measuring the extent to which platformization is contributing to economic growth in Canada. Sharing or other platform business practices may be much more widespread than we know, and would certainly be misrepresented by the activities of just two specialized services (peer to peer ride-sharing and private accommodations).

These observations reinforce the approach to digital innovation being proposed by Canadian industry and the federal government, which is to translate new innovations in digital technology, particularly those that center around big data, into other sectors of the economy. The goal is for Canada's traditional economic sectors to establish new competitive advantages through the uptake of new business processes so that they remain competitive in the global economy. Note that, for this strategy to work, Canada need not assume the risk of developing new digital economy business practices – it just needs to figure out how to incorporate those practices into its flagship industries in impactful ways. This rapid adaptation and uptake of foreign (especially American) innovations is a recognized Canadian strategy for economic development, which explains why R&D investments by Canadian industries are consistently lower than those of their American counterparts.[11]This suggests that platformization (here defined as the adaptation of platform business practices to the Canadian business context)

7 https://www.ic.gc.ca/eic/site/693.nsf/eng/00157.html

8 https://www.statcan.gc.ca/daily-quotidien/170228/dq170228b-eng.htm

9 http://www.cmcrp.org/the-growth-of-the-network-media-economy-in-canada-1984-2016/

10 https://www.statcan.gc.ca/pub/13-605-x/2017001/article/14771-eng.htm

11 https://nationalpost.com/news/politics/canada-has-failed-at-innovation-for-100-years-can-the-trudeau-government-change-that

will be a central aspect of Canada's innovation strategy, and as such, that it will have significant implications for how data policies are reformulated in the future.

Meanwhile, changes in international policy are putting pressure on federal regulators to reexamine their approach to the regulation of data. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) – the main legal framework regulating personal information – came into effect in 2000. Its primary *raison d'etre* was to support Canada's trading relationship with the European Union (EU). PIPEDA allowed Canada to achieve 'adequacy status' under the EU's 1995 Data Protection Directive, which regulates the conditions under which EU data can be legally transferred to foreign countries. Under the EU's new General Data Protection Regulation (GDPR), which came into force in May 2018, not only can adequacy be reviewed (and repealed) but the provisions used to judge adequacy have changed. In addition to the GDPR's old principles of purpose limitation, data quality and proportionality, transparency, security, rights of access, rectification and opposition, and restriction of onward transfers, the GDPR now also adds the principles of data breach notification, the right to be forgotten, the right of data portability, and, privacy by design and by default.[12]

Canada's current legal framework falls short on all of these new provisions, except data breach notification, which was strengthened through the 2015 Digital Privacy Act (an amendment to PIPEDA). This raises the possibility that Canada may lose its adequacy status during upcoming reviews. If this happens, Canadian firms would need to demonstrate their compliance with European law through contract negotiations, which would create a barrier to the creation of transatlantic business partnerships. For the moment, Canada appears to be waiting things out to see whether and how the new regulations are implemented, and with what affects for Canadian businesses.

Meanwhile, Canada is also involved in important trade (re)negotiations including the Comprehensive Economic Trade Agreement (CETA) with the EU, the Trans-Pacific Partnership (TPP), and the renegotiation of the North American Free Trade Agreement (NAFTA). CETA's main data provisions appear in its section on e-commerce, which states, "Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards of data protection of relevant international organisations of which both Parties are a member" (Article 16.4). The adequacy framework described above helps us understand why this provision is sufficient to secure an agreement about movement of data between Canada and the EU.

The text of the TPP includes similar provisions in Article 14.8 on personal information protection, and it also includes additional provisions on 'Cross Border Transfer of Information by Electronic Means' in Article 14.11. Here, the TPP says, "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." This is a reference to the issue of data-localization. The GDPR allows for transfer of the private data of EU citizens when the adequacy of the data-receiving jurisdiction is recognized. But the TPP reveals Canada's long-standing position on localization of private data of Canadian citizens, which is that localization should only be required for government data[13],

however processing and management of personal data held by federal agencies can be outsourced, provided it does not threaten the data rights of citizens.[14] This issue has also arisen in NAFTA negotiations. In this case, the treaty language actually places limits on any efforts to restrict data flows.[15] As Canadian academic Michael Geist

12 http://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-new-general-data-protection-regulation/

13 http://www.michaelgeist.ca/2017/12/canadian-position-data-localization-rules-trade-deals-revealed-protection-government-data/. The Privacy Act (not PIPEDA) governs the use of personal data by federal government institutions, as well as rights of access to personal information held by federal agencies. The Privacy Act was established in 1983, and emerged out of constitutional law (the Canadian Human Rights Act of 1977 and the Canadian Charter of Rights and Freedoms of 1982) which established norms around "security of person" as well as "freedom from unreasonable search and seizure." The Privacy Act created the Office of the Privacy Commissioner. The Access to Information Act provides broader rights to access information under federal government control.

14 https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/

15 http://www.michaelgeist.ca/2017/04/deciphering-u-s-nafta-digital-demands-part-two-digital-economy-services-transparency/

points out, "Given that data often ends up in the United States, restrictions on data localization requirements have emerged as a key US demand in its trade agreements."[16] To this we would add that given how Canadian companies seek to adapt US strategies to the Canadian marketplace, caving in to American data localization restrictions makes perfect sense.

Considering these various pressures, arising both domestically (from innovation policy) and internationally (through trade policy), there is growing interest in a general review of data policy in Canada. In a January 2018 Toronto Star opinion piece, Jim Balsillie of Blackberry fame said, "It's critical that Canada designs and implements a National Data Strategy to protect our prosperity, security and values." And in February 2018, Rohinton P. Medhora, President of the Canadian Centre for International Governance Innovation (CIGI) hosted a closed-door round table with Chrystia Freeland, Minister of Foreign Affairs and David Lametti, Parliamentary Secretary to the Minister of Innovation, Science and Economic Development to spark interest in the development of just such a strategy. CIGI simultaneously released a report called, "A National Data Strategy for Canada: Key Elements and Policy Considerations" which says, [17]"Canada's national data strategy must begin drafting the terms of a new social contract between citizen providers of data and those in industry and government who want to collect and use it" (Medhora 2018, p. 8). Finally, a February 2018 article in the Globe and Mail reported that the Council of Canadian Innovators is calling for a National Data Strategy, and that various actors hoped the Canadian government would include money for this work in the 2018 federal budget.[18] (This article again makes the link between data, innovation and Canada's resource sectors.)

Considering the various pressures, arising both domestically (from innovation policy) and internationally (through trade policy), there is growing interest in a general review of data policy in Canada

The requested monies did not materialize in the 2018 budget, but all the same, the momentum towards a review of Canada's regulatory framework for data seems to be growing. Any effort to reorient the data policy framework in Canada will certainly have implications for platform-based enterprises and platform business strategies.

In what follows, we explore the intentions and limitations of the existing data policy framework in greater detail and we identify the key players and discourses at work in the data policy community in Canada, as well as examine some of the main issues that will shape debate on the development of a new data policy framework in the country.

For our purposes, the key data policy in Canada is PIPEDA, the above mentioned Personal Information Protection and Electronic Documents Act. It is accompanied by the Anti Spam Legislation, CASL. These two policies are the main frameworks directly affecting the use of personal information by private sector companies in Canada. The country's larger data regime includes a Privacy Act (R.S.C., 1985, c. P-21), which addresses management of private data by the federal government, as well as access to information laws, and freedom of information laws. Canadian governments at the federal, provincial and local levels also have a variety of different open government data policies.[19] Canada has a strong apparatus for regulating the management of data used for government-funded research.[20] It also has several subsidiary and sectoral privacy laws that address specific privacy concerns. For example, four provinces have health-related privacy laws, and the Bank Act (which regulates the banking sector) also contains provisions about data and privacy. While these policies could all have implications for private

16 http://www.michaelgeist.ca/2017/12/canadian-position-data-localization-rules-trade-deals-revealed-protection-government-data/
17 https://www.cigionline.org/sites/default/files/documents/Paper%20no.160_3.pdf
18https://www.theglobeandmail.com/news/national/canadian-ceos-and-academics-push-ottawa-for-national-big-data-strategy/article37848737/
19 See for example the main page of the federal open data portal: https://open.canada.ca/en/open-data
20 http://www.science.gc.ca/eic/site/063.nsf/eng/h_83F7624E.html?OpenDocument

companies in specific circumstances, we will not address them here, choosing instead to focus on the policies that establish Canada's primary approach to regulating data in the commercial realm.

PIPEDA and CASL emerged with the rise of the internet and were passed to support the growth in electronic commerce both domestically, and (as explained above) internationally. Prior to this, privacy was protected against the backdrop of the Canadian Charter of Rights and Freedoms and was interpreted to be "an essential component of individual freedom."[21] This framework was increasingly used as the basis for legal challenges against data use by private companies in the 1990s. As a result of this, in 1995 the Canadian Standards Association published a Model Code for Protection of Personal Information as a framework for business self-regulation. This framework then became the basis for PIPEDA.

"Based on a conception of privacy as an individual human right, the paradigm shaped the landscape for protection in terms of the basic principles outlined in leading documents such as the 1980 OECD Guidelines and the 1981 Council of Europe Convention 108. The paradigm enjoined data controllers to fulfill certain obligations and gave rights to data subjects that could form the basis for complaints to regulatory agencies (e.g., data protection authorities) and ultimately for litigation. The context for the paradigm was a much simpler information environment than has evolved since the 1980s. It was one in which individuals as citizens and consumers could realistically aspire to "informational self-determination", although in most cases that aspiration remained a forlorn hope." (Bennet & Raab, 2017)[22]

It is important to note that PIPEDA centers around "personal information" which it defines in this particular way- "information about an *identifiable* individual, but does not include the name, title or business address or telephone number of an employee of an organization" (emphasis added). This definition provides the basis for an important loophole where anonymization is concerned, which we will revisit below. The law establishes a consent-based framework for private sector collection, use or disclosure of personal information. It provides citizens with the right to know why a private sector actor is collecting, using or disclosing personal information, the right to obtain access to their personal information, and, if they wish, the right to correct or update that information. It also states that companies may not use information for purposes other than that for which consent was obtained. PIPEDA has been amended once, in 2015, through the Digital Privacy Act, to regulate mandatory disclosures of privacy breaches.

PIPEDA's regulatory framework does not provide the means to directly sue companies that violate its terms. Instead, it has created the Canadian federal Office of the Privacy Commissioner (OPC), which has a duty to receive complaints from citizens with regards to breaches of their personal information rights, and to investigate those complaints. It also has a responsibility to educate businesses and the public, and to recommend criminal investigations or prosecution should it feel there is merit in doing so. This means that Canada's Federal Privacy Commissioner, Daniel Therrien, can investigate privacy concerns that fall within the ambit of PIPEDA, and he can recommend criminal investigations, or pursue court action, but he has no powers of enforcement. It also means that PIPEDA is updated via judicial interpretation and the production of case law.

The enforcement mechanisms contemplated by PIPEDA are balanced off by self-regulation on the part of private sector actors, who have taken the lead in developing best practices and technologies that facilitate the adoption of PIPEDA's mandates in their everyday business activities. In addition, Canadian private sector actors have adopted additional tools to demonstrate compliance with the law, such as privacy impact assessments (Beyley and Bennett,

21 Communications, Government of Canada, Department of Justice, Electronic. "Department of Justice - THE OFFICES OF THE INFORMATION AND PRIVACY COMMISSIONERS: THE MERGER AND RELATED ISSUES". www.justice.gc.ca.
22 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086

2012).[23] PIPEDA's philosophy can be summarized by four concepts: privacy of personal information, consent as a basis for use by third parties, self-regulation by third parties, and citizen-driven enforcement of the law.

PIPEDA's companion, CASL, was not introduced into law until 2014, and was the culmination of a protracted battle to relieve citizens of unwanted intrusions by private sector companies. Canadian companies had long argued that if a person made their contact information public, then companies should have the right to use it to advance their business interests. Citizens, on the other hand, argued that unwanted phone calls or emails were an invasion of their privacy. CASL ushered in permission-based marketing in Canada, which represented a compromise. Under CASL, companies must have explicit consent before sending commercial electronic messages, installing computer programs, or collecting personal information. The privacy commissioner has some responsibility to govern CASL, however, it is primarily enforced by the Canadian Radio-television and Telecommunications Commission (CRTC), and in this case, the CRTC has the power to levy monetary penalties against companies that violate the law. This is telling, because while PIPEDA applies to all business interests in Canada, it is apparent from the way CASL is implemented that it primarily focuses on media companies. As we shall see, this distinction may be breaking down in the Canadian case where the platform economy is concerned.

2.1 Canada's Existing "Personal Information" Policy Community

Canadian governance is known for having a strong liberal democratic compromise, and policymaking at the federal level is marked by the involvement of policy communities.[24] That is, federal policymaking is characterized by relatively stable groups made up of government actors and public interest groups who negotiate over policy and implementation in a field of shared interest. This is similar to the approach to governance seen in other Westminster style democracies such as the UK and Australia. According to interviewees, the personal data policy community in Canada is a relatively collegial ambit that convenes around three main spaces: the Office of the Privacy Commissioner (OPC), the House of Commons (which calls on actors to address parliamentarians when it conducts periodic legal reviews), and the CRTC. As academician Colin J Bennett explains, these groups are characterized by their legal expertise and professionalism, and there is little involvement from the larger publics in these spaces:

> "In most countries, there is still, therefore, a dominance of legal reasoning and scholarship within the literature. One reason, I suggest, is that policy instruments have spread, and the policy community expanded without significant intervention from mass publics, political parties or interest groups. As with other questions associated with the communications and information revolution, whether it be broadcasting, telecommunications regulation, freedom of information, or intellectual property, these issues tend to be seen as within the more specialized and technocratic realms of policy making and administration. For the most part they do not excite passions and adherence. They rarely appear in party platforms. And they seldom affect the election or dismissal of elected officials" (Bennett, 2011).[25]

23 https://link.springer.com/chapter/10.1007/978-94-007-2543-0_7
24 https://www.canada.ca/en/privy-council/news/2017/03/clerk_s_remarks_atthepolicycommunityconference.html
25 https://www-tandfonline-com.proxy.lib.sfu.ca/doi/full/10.1080/13876988.2011.555996?scroll=top&needAccess=true

Overall, there are several 'big wave' discussions which tend to set the parameters for the 'little wave' debates within the space. 'Big wave' discourses are world views of the actors, while 'little wave' discourses are their responses to specific privacy-related issues that arise in the Canadian polity.

Based on an analysis of House of Commons hearings, a review of newspaper articles, and interviews with public intellectuals in Canada, we conclude that this space has tended to organize itself into four main groups: representatives of business in the broad sense, representatives of media industries more specifically, public interest groups, and, academics. Table 1 provides a taxonomy of these groups. Within this community, the media industry has played a particularly prominent role, including the traditional "broadcast distribution units" (BDUs) as they are known by the CRTC, and also the new digital media players. This makes sense, since their main interest in collecting personal data lies in selling it to actors who wish to influence people's preferences in the marketplace or the political sphere. Privacy policy sets the conditions under which they can engage in this business enterprise. Whether they are broadcasters, social media players or telcos, the game is the same, and they find themselves in direct competition with each other.

Table 1: "Personal Information" Policy Community in Canada

Industry groups	Media industries	Public interest groups	Academics
Representatives of companies that use data in their industrial or communications practices.	Representatives of media industries that are specifically focused on communications activities.	Civil society or consumer protection groups who advocate on behalf of the public.	Researchers and public intellectuals who follow and comment on data policy issues.
Canadian Chamber of Commerce Retail Council of Canada Canadian Bankers Association Canadian Life and Health Insurance Association Insurance Bureau of Canada National Association for Information Destruction Law firms representing business interests	Facebook, Google, ISPs, Telcos / BDUs Canadian Marketing Association (CMA) Canadian Wireless Telecommunications Association (CWTA) Information Technology Association of Canada (ITAC) Interactive Advertising Bureau of Canada (IABC)	Public Interest Advocacy Centre (PIAC) BC Freedom of Information and Privacy Association (BC FIPA) Canadian Internet Policy and Public Interest Clinic (CIPPIC) Citizen Lab Open Media Centre for Law and Democracy, etc.	Michael Geist Fenwick Macklvey Teresa Scassa Colin Bennett, Ian Kerr, Jane Bailey, etc.

The policy community around personal information has been characterized by a series of issues that establish the parameters of its debates. These are listed in Appendix A. Overall, there are several 'big wave' discussions which tend to set the parameters for the 'little wave' debates within the space. 'Big wave' discourses are world views of

the actors, while 'little wave' discourses are their responses to specific privacy-related issues that arise in the Canadian polity.

One of the most important 'big wave' discussions centers around whether the Canadian privacy regulatory framework is essentially workable, or whether it has fundamental flaws that render it ineffective and in need of reform. These debates take up the ability of the legal framework to protect the privacy of citizens, as well as the nature of the implementation and enforcement regime. In general, actors from the private sector and industry associations argue that PIPEDA is a good law that meets the demands of industry and privacy rights, and facilitates self-regulation.[26] However, public interest groups, academics and the privacy commissioner of Canada are of the opinion that PIPEDA needs to be legislatively revised and "modernized[27]". Here, the arguments range from making tweaks to PIPEDA, to wholesale reconsideration of the law, while suggestions move from recognizing how the privacy landscape has changed, and Canada's need to adapt to these changes through specific, privacy-related reforms, to larger reviews of a wider spectrum of data and consumer protection laws. Forexample, Teresa Scassa from the University of Ottawa told the House of Commons Committee in 2012 that "the collection, use, and disclosure of personal information is no longer simply an issue of privacy, but also raises issues of consumer protection, competition law, and human rights, among others". As such, "data protection law reform is overdue and may now require a reconsideration or modification of the consent-based approach, particularly in contexts where personal data is treated as a resource and personal data collection extends to movements, activities, and interests.[28]"

Within this space we see many 'little wave' discussions as well. One of them relates to the privacy commissioner's lack of enforcement powers versus the desire of the industry to self-regulate. Public interest groups, academics, and federal and provincial privacy commissioners believe that the OPC should have stronger enforcement powers. These actors have noted that PIPEDA compliance by organizations has remained problematic because non-compliance carries minimal risk[29] – that PIPEDA "has no teeth."[30] These groups also suggest that the privacy commissioner should have stronger abilities for levying financial penalties and fines in case of compliance failures. However, private sector associations consider that accountability frameworks based on self-regulated industry standards and codes of conduct are preferable over legislated obligations, and that "a collaborative relationship between industry and the regulator is more efficient, and results in better outcomes for consumers.[31]"

Another 'little wave' debate focuses on whether the existing consent model is adequate or whether it has problems. Public interest groups, academics and privacy commissioners consider that, in an era of big data and the Internet of Things, individuals do not always give meaningful or valid consent to all business-related activities that involve their personal information.[32] These groups also manifest that companies should improve transparency in their data management and algorithmic decision-making processes, since "transparency is at the heart of the consent-based data protection scheme.[33]" Tamir Israel from the Canadian Internet Policy and Public Interest Clinic

26 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.31.

27 Testimony by Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada) House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 46. February 16, 2017. pp.2-3.

28 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013 p.33.

29 Testimony by Mr. Dennis Hogarth (Vice-President, Consumers Council of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 61. Tuesday, May 16, 2017. p.3.

30 Canada's privacy watchdog seeks stronger enforcement powers Krashinsky Robertson, Susan . The Globe and Mail ; Toronto, Ont. [Toronto, Ont]22 Sep 2017: A.1.

31 Testimony by Mr. Robert Ghiz (President and Chief Executive Officer, Canadian Wireless Telecommunications Association). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 60. Thursday, May 11, 2017. p.4.

32 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.31.

33 Testimony by Prof. Teresa Scassa (Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49 February 23, 2017. p.3.

(CIPPIC) considers that "the modern era had strained consent as one of PIPEDA's core pillars", and that this strain arises from "the increasingly complex nature of modern data practices, which in turn leads to opaque data capabilities, powerful incentives that are often directly at odds with those of consumers, and inaccessible privacy policies that seek either to capture this complexity, or at the other extreme, to obscure it in order to maintain flexibility for future organizational practices.[34]" Geist considers that, given the uncertainty associated with big data and cross-border data transfers, "new forms of transparency and privacy policies are needed". Geist suggests that, for example, "algorithmic transparency would require search engines and social media companies to disclose how information is used to determine the content displayed to each user", while "data transfer transparency would require companies to disclose where personal information is stored and when it may be transferred outside of the country.[35]"

Industry responses to these concerns note that data anonymization is one of the ways to surpass the problems with obtaining meaningful or valid consent, while others push for the implementation of a risk assessment-based model. Anonymization, also called de-identification or obfuscation, "protects individuals because the data can be rendered non-identifiable.[36]" However, public interest groups argue that anonymization "is not a panacea for the current privacy concerns", in part because "as anonymization gets stronger, the commercial value of information can often decline, giving businesses an incentive to pursue incomplete solutions.[37]" Private sector representatives also suggest the adoption of risk-based approaches and more implied consent frameworks. This solution responds to the limitations of garnering express consent in today's fast-paced internet, "including individuals' willingness to read or understand what they are consenting to.[38]" A risk-based approach or interpretation would focus on obtaining express consent only for data collections, uses, or disclosures of personal information, if such activities might trigger a risk of harm to individuals (such as making an eligibility decision impacting the person, a disclosure that would involve sensitive or potentially embarrassing information, or a practice that would go against the expectation of the individual).[39] However, public interest advocates manifest against this risk-based accountability framework because "it would effectively amount to open season on individual data.[40]" As the opposite solution, John Lawford from the Public Interest Advocacy Centre believes that "PIPEDA needs to enable the informed consent standard, and all it needs is some new rules to protect that and consumers.[41]"

Overall, industry actors state that collecting and analyzing consumers data benefits Canadian businesses and consumers alike. Some of its derived provisions such as targeted or online behavioral advertising "can reduce the time consumers spend looking for products by focusing on the things of most interest to them[42]", while data analysis leads to increased revenues and competitive advantage for companies. Academics such as Teresa Scassa, Ian Kerr and Jane Bailey, however warned about profiling as a by-product of big data analytics with implications for human rights, especially discrimination. Profiling as "the placing of users, accurately or inaccurately, into social

34 Testimony by Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.3.

35 Testimony by Dr. Michael Geist (Canada Research Chair in Internet and Ecommerce Law, Professor of Law, University of Ottawa, As an Individual). Testimony by Mr. David Fraser (Partner, McInnes Cooper, As an Individual). House of Commons Canada.

36 Testimony by Mr. Adam Kardash (Partner, Privacy and Data Management, Osler, Hoskin and Harcourt LLP, Interactive Advertising Bureau of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 62. May 30, 2017. p.7.

37 Testimony by Mr. Michael Karanicolas (Senior Legal Officer, Centre for Law and Democracy) House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.2.

38 Testimony by Mr. Robert Watson (President and Chief Executive Officer, Information Technology Association of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 61. May 16, 2017. p.2.

39 Testimony by Dr. Éloïse Gratton (Partner and National Co-Leader, Privacy and Data Protection Practice Group, Borden Ladner Gervais, As an Individual). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 46. February 14, 2017. p.5.

40 Testimony by Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.3.

41 Testimony by John Lawford (Executive Director and General Counsel, Public Interest Advocacy Centre). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 46. February 14, 2017. p.3.

42 Testimony by Mr. Jason McLinton (Vice-President, Grocery Division and Regulatory Affairs, Retail Council of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 63. June 1st, 2017. p.5

categories…on the basis of information processing[43]", can be used to characterize individuals as "unworthy of special discounts or promotional prices, unsuitable for credit or insurance, or uninteresting as a market for particular kinds of products and services.[44]" Profiling is another argument within the call for greater corporate transparency and the 'big wave' discussion on whether the existing legal framework is fully able to protect the privacy of Canadians.

A second 'big wave' concern revolves around data jurisdictions, including both the negotiation of relationships with other jurisdictions, as well as Canada's long-standing commitment to a policy of data responsibility instead of data localization. (Companies are responsible for ensuring that the data they manage adheres to Canadian law even when it passes into other jurisdictions.) Debates here include whether PIPEDA should be modernized to meet the standards of the EU's new GDPR. Specifically, privacy commissioners, some public sector organizations and "industry observers[45]" believe that Canada should modernize its privacy laws to maintain the country's status as an adequately protected jurisdiction for harboring European data. However, private sector representatives argue that making such legislative changes in PIPEDA would be "premature", and that "a more precise view may be revealed going forward as we have more experience with the GDPR and its transborder adequacy review process.[46]"

Other debates focus on data localization and cloud-computing. Public interest groups and academics manifest that this creates concerns vis-à-vis the problems of holding jurisdictional control over private data of Canadians stored outside the country. PIPEDA does not prohibit organizations from using cloud service providers that store personal information outside Canada, thus companies often reduce costs and ease processes by storing data off site or outsourcing software functions. PIPEDA only recommends that the privacy risk be identified, including the need for transparency, consent, and notification of the individual the personal information is about. Greg Kozak of the Association of Canadian Archivists expressed that his organization "believes that PIPEDA should make a definite statement on the issue of the jurisdictional location of data of private individuals; otherwise, what happens to them will be mostly be decided by legal opinion rather than by clear, consistent rules.[47]"

When debates arise over these concerns, actors rely on certain discourses to curry favor or attract followers to their side. Discourses at work in the existing policy space include those around good corporate citizenship with businesses portrayed as essentially good and in the service of the country. For example, private sector and industry representatives often refer to the "dramatic"[48] and "continued"[49] growth of Canada's digital economy and ICT sector (which is "attracting millions of dollars of investment… and is creating thousands of jobs in Canada"[50]), and use the term "collaboration[51]" when referring to the existing and desired relationships between industry and regulators. They also speak of the "benefits"[52] of business practices in collecting personal information not only for

43 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. pp.9-10.

44 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. pp.9-10.

45 Calls grow for Canada to modernize privacy laws. Krashinsky Robertson, Susan. The Globe and Mail ; Toronto, Ont. [Toronto, Ont]24 July 2017: B.1.

46 Testimony by David Young (Principal, David Young Law, As an Individual). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 54. April 4, 2017. p.2.

47 Testimony by Mr. Greg Kozak (Representative, Ethics Committee, Association of Canadian Archivists) House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 63. June 1st, 2017. p.4.

48 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.4.

49 Testimony by Mr. Robert Watson (President and Chief Executive Officer, Information Technology Association of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 61. May 16, 2017. p.2.

50 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.4.

51Testimony by Mr. Robert Ghiz (President and Chief Executive Officer, Canadian Wireless Telecommunications Association). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 60. Thursday, May 11, 2017. p.4. / Testimony by Mr. Robert Watson (President and Chief Executive Officer, Information Technology Association of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 61. Tuesday, May 16, 2017. p.2.

52 Testimony by Mr. Jason McLinton (Vice-President, Grocery Division and Regulatory Affairs, Retail Council of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 63. June 1st, 2017. p.5

organizations but also for consumers (such as with targeted advertising), and of having a commitment with "enhancing privacy protections for individuals."[53] For example, representatives of the Canadian Marketing Association (CMA) have explicitly stated that "legitimate businesses have every incentive to anticipate consumer privacy needs and resolve any concerns."[54]

However, other discourses around consumers' protection and privacy rights portray businesses in a negative light. As mentioned above, public interest groups and academics speak of the "lack of openness" or "transparency"[55] by companies, while the term "black box"[56] is also used to speak about data management practices by corporations. Privacy policies are seen as "inaccessible," "impractical" and "unrealistic" for users to read,[57] and data processes as "opaque" and "obscure."[58] Results of data aggregation such as profiling are described as "discriminatory"[59] and a source of exclusions and privileges.[60] This builds on an overarching discourse of businesses versus consumers where "powerful [corporate] incentives" are described as "often directly at odds with those of consumers."[61] Moreover, businesses are portrayed as acting on their self-interest in the pursuit of economic gains. For example, "social media companies and other information brokers will partner with whoever they want to in order to make lucrative arrangements."[62]

The "personal information" policy community is structured around established institutional and discursive spaces: PIPEDA and its provincial adaptations, plus a narrative about the tensions that exist between private gain and personal protection

Overall, the "personal information" policy community is structured around established institutional and discursive spaces: PIPEDA and its provincial adaptations, plus a narrative about the tensions that exist between private gain and personal protection. The institutional space and discursive space can be seen as complementary, since the OPC precisely exists to adjudicate said tensions. But as we see signals of a broader data policy landscape emerging in Canada, it is possible to think that other communities of actors are also multiplying across a wider spectrum of policy fields.

53 Testimony by Mr. Wally Hill (Vice-President, Government and Consumer Affairs, Canadian Marketing Association) House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 60. May 11, 2017. p.4.

54 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.5

55 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. pp.9-10.

56 Testimony by Prof. Jane Bailey (Professor, Faculty of Law, University of Ottawa, As an Individual). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 68. September 25, 2017. p.2.

57 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.9. / Testimony by Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.3.

58 Testimony by Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.3.

59 Testimony by Prof. Jane Bailey (Professor, Faculty of Law, University of Ottawa, As an Individual). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 68. September 25, 2017. p.2.

60 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.10.

61 Testimony by Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.3.

62 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.9.

3. Canada's Emerging Data Policy Landscape

While data policy was nearly synonymous with privacy policy in Canada for a long time, today, it is not. Our sense is that the original discussion of data policy in Canada centered around privacy rights and therefore the primary community was made up of privacy actors. To complicate matters, Bennet observes that privacy advocates were rarely focused only on privacy. They usually arrived at privacy via other broader concerns related to civil rights, human rights, consumer freedoms or digital freedoms.[63] But having said this, these actors have had a relatively cohesive set of concerns that revolved around an individually-based consent model, and bureaucratic approaches to privacy compliance.

Today this focus is coming under stress for a series of reasons. The first set of reasons involves a transformation in the privacy space itself. Bennet and Raab[64] argue that there are four main sources of pressure on privacy policy. First, the top down model of oversight by privacy commissioners is increasingly being replaced by business-driven accountability models, often based on technological solutions. Second, there is a growing concern about the ethical dimensions of privacy law, particularly since so much data is collected about people through surveillance, that is not necessarily individually identifiable, often without awareness, and for purposes that we do not know. Third, the individualistic focus of consent-based models is being questioned on the basis of broader societal concerns as people begin to ask about the value of privacy to the larger economy and community. And finally, companies are increasingly driven by the desire to manage risk, because when they get privacy wrong they find that their valuations rapidly fall (as was Facebook's experience with Cambridge Analytica). And yet Bennet still believes that privacy and consent are essential to data governance because from his point of view there is no 'big data' without people's consent to share their information. And so for him, consent remains at the heart of data regulation, and privacy policy is the anchor of all other data-related policies.

Others disagree, especially given recent debates over the relative importance of data privacy and data protection. Data protection is not about consent, they say, but rather focuses on securing a resource that has already been collected. It reflects the fact that privacy may not be very relevant to a generation of people who have always given their personal information away, and that people give their information away all the time, whether or not they even realize it. Data security opens the door to the possibility that data can be collected without consent, as long as it is properly managed once collected. This agenda reflects the growing recognition that data is a resource that confers significant economic and political advantages on the people who hold it, and that it has become a valuable foundation for innovation and the establishment of competitive advantages in the global economy. This would also explain why there is an increasing tendency to apply intellectual property law to collections of data. So while some argue that data privacy and data protection are overlapping and complementary[65], in our view, they evidence the emergence of tensions within data regulatory frameworks.

In the Canadian case, these changes are reflected in the emergence of new pockets of discussion about data policy that are taking place in disparate spaces, such as conferences on innovation, the digital economy, intellectual property, trade, and the like. We are beginning to see specific examples of these spaces such as the recent Annual Partnership Network Conference of the Creating Digital Opportunity (CDO) – an initiative based at the University of Toronto - which was held in Vancouver in April 2018. This conference featured extensive discussions about Big Data's role in innovation, in the context of the new Digital Technology Supercluster initiative. This is particularly

63 "Virtually every group mentioned so far has been involved in Internet privacy questions. Some, however, have emerged solely as a result of the Internet and from desires to create an open medium based on sound democratic principles. The existence of a separate set of "digital rights" which are an extension of more fundamental civil rights and liberties is controversial. The belief, however, frames the work of a number of national and international organizations, of which the Electronic Frontier Foundation (EFF) is probably the most important."
https://www-tandfonline-com.proxy.lib.sfu.ca/doi/full/10.1080/13876988.2011.555996?scroll=top&needAccess=true
64 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086
65 https://blog.ipswitch.com/data-privacy-vs-data-protection

interesting since the CDO is headed by Dr. David Wolff, a global expert on technology clusters and innovation. The event brought together academics and industry leaders to position possible future directions for data policy.

Even the privacy policy community has noted the need to expand the discussion to other areas. In the debates about whether to modify PIPEDA vis-a-vis the GDPR, a representative of the Canadian Chamber of Commerce noted that "we must understand that the GDPR is much broader than just privacy. It's as much about the public sector and security as it is about privacy,"[66] while Scassa has also remarked on Canada's need to adapt to current scenarios through larger reviews of a wider spectrum of data, consumer protection, competition and human rights laws.[67] When RightsCon was held in Toronto in May 2018, it offered an opportunity for Canadian NGOs to come together around these issues for the first time. The concerns of this group are principally centered around citizen rights in the face of the Internet of Things and Big Data as they are expressed in and through urban planning (smart cities). As a result of this, the Vancouver-based NGO Open Media and the Ottawa-based NGO, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) are proposing a national meeting of civil society groups, and a leading voice, Bianca Wylie from CIGI, has launched a petition to gather support for a national data strategy at the end of June 2018 ().[68] This call notably suggests that the topics up for discussion include, "data collection, ownership, use, and rights; privacy as a public good; consent; equitable internet access; fair competition; and, future prosperity." These issues clearly extend beyond the existing privacy policy landscape. Indeed, parallel spaces have become key spheres of debate about data issues - such as IP (ownership of data), competition, human rights/ digital rights, innovation, infrastructure (cloud etc.), trade/localization, among others.

In total, we are seeing the privacy policy community, with its established government ties, come to be eclipsed by a broader data policy advocacy network, that does not yet have strong ties with government. And the wider data policy advocacy network is raising a host of new issues that may be decentering the importance of privacy and consent. We summarize these issues here by examining how platform data is running up against existing legal frameworks:

3.1 Competition Law

Companies have long gathered intelligence about their client base. But platform-based practices may make it possible for companies to gather or acquire information about their clients in new and concerning ways. For example, the knowledge that companies amass about their clients may enable them to engage in anti-competitive pricing practices, or forced loyalty schemes. CIGI points out, "Data holdings are now a key element of a business's ability to dominate a market and stifle competition" (CIGI, page 10).

3.2 Intellectual Property Law

This law is also relevant to digital platform practices. In 2016, as reported by Scassa, a Canadian court upheld a decision to apply copyright protections to a compilation of data, as if this data were a cultural product (such as a book or a movie). The application of copyright law to databases of consumer data would provide companies with a tool to avoid public scrutiny of their data practices. In addition, enhanced copyright may not be in the best interest, "For example, while content industries might consider increased protection for technological protection measures -- or 'digital locks' -- to be essential in the fight against unauthorized copying, the same protection, when applied to

66 Testimony by Mr. Scott Smith (Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 61. Tuesday, May 16, 2017. p.5.

67 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013 p.33.

68 https://digitalrightsnow.ca/

compilations of data, could have the effect of overriding the basic copyright principle that facts are in the public domain" (CIGI, page 11).

3.3 Data as a Resource

There is also the suggestion that federal actors are taking an interest in updating Canada's innovation, labor and taxation policies to reflect new business practices. Statistics Canada is considering how to update national accounts to better capture the economic value of these activities. And, the 2018 Canadian Internet Use Survey includes questions about the use of platforms to supplement or replace traditional labor activities. This research raises new questions, such as: What is the value of data assets held by Canadian companies? Should they be included in corporate income tax filings? What supports or protections should the federal government offer to Canadian workers? How is innovation changing, and should incentives change to reflect new and different approaches production?

This also has implications for Canadian innovation policy. A recent report by CIGI argues, "Growing Canada's share of global data capital – and therefore broadening its stake in the global data-driven economy – will depend heavily on the extent to which Canadian firms can capture data in areas where first movers have not already established insuperable dominance." It goes on to say that, "in some instances, private sector-led commercialization may be optimal; in others, it might be better to make data available to the public at sub-market prices. Above all, decision makers need to recognize and account for the potential use and exchange value of this data when developing and implementing policy." (page 2). These comments help us understand how Canadian innovation policy will adapt platformization into markets that are not already dominated by established actors. Trudeau's innovation policy has taken up health, mining and agriculture as key areas to focus on.

4. Considerations for Data Policy Moving Forward

Despite these pressures, there is currently no indication that Canada will engage in broad-based changes to its national data policy framework. But there are definitely suggestions that the broader conversation around data is changing, and that the existing privacy policy community is being displaced as the primary and only ambit of discussion about private sector data use. Meanwhile, policies are always shifting in minor ways with changes in context and the emergence of new implementation strategies. In this section we suggest some of the issues that should be taken into consideration as Canadian data policy shifts and changes.

4.1 Data versus Algorithms

Algorithms are fundamentally changing the game where data is concerned. The PIPEDA framework was created to protect private information and is based on a fundamental distinction between private and public information. Unfortunately, it has been relatively simple for private sector actors to circumvent PIPEDA by anonymizing data. If the data is anonymous, they argue, then it no longer infringes on privacy. The difficulty here is that algorithms make it relatively easy to deanonymize data. This means that algorithms take us into an entirely new realm, requiring new approaches to privacy law and digital rights. This is the primary reason why Canadian data policy may need to consider taking up data protection issues in addition to data privacy issues, beyond simply a desire to comply with the GDPR.

4.2 Types of Data

When creating data policy, we need to categorize data according to its functional purpose. Based on our observations about the Canadian case, we believe it is important to distinguish between data that is used to influence people's preferences and data that is used to intercede in intermediation of goods and services. Data intensive companies that make money by giving away entertainment services, and then selling advertising, use data primarily to drive targeted marketing. But platform intermediaries use data primarily to govern the terms of interaction within a marketplace. This means that the use value of the data is different depending on the business strategy at work in each case. This is why we are seeing different policy discussions emerge around competition policy versus intellectual property law, for example. In the former case, the challenge is to regulate data's contributions to monopolistic tendencies. In the latter case, the challenge is to determine who owns data, and whether something like an 'end user license agreement' (EULA) works to dispossess users of their property. [69]

In the Canadian case, the networked media economy, as Dwayne Winseck calls it,[70] is the most vocal when it comes to regulating private data. This group includes both traditional 'broadcast distribution undertakings' (Bell, Rogers, Corus/Shaw, Quebecore) as well as new media actors such as Facebook and Google. What unites them is a desire to influence people's preferences so that they will be more inclined to engage in particular types of buying or voting behaviors. But making the final choice is left up to the consumer or citizen in a market place that offers multiple options. These groups have a huge stake in maintaining a ready flow of personal data to drive their advertising activities.

On the other hand, businesses that engage in platform-based intermediation of goods and services have stayed quiet in Canadian policy circles that address data-related issues. Why is this? We surmise that it is because these actors view their data as a source of competitive advantage, so they are not inclined to share it with others.[71] Ergo, privacy laws are less of a concern to them. In addition, the data is collected under conditions that will necessarily engender the user's consent, so PIPEDA is generally an agreeable policy framework for these actors. In other words, as long as they ask permission from users, and have them sign an EULA that dispossesses them of their data, the companies have no need for legal reforms. Indeed, they would likely avoid starting any kind of debate that might lead to enhanced rights for data sources.

This does not mean that the data-intensive practices of platform intermediaries are beyond regulatory scrutiny. Trade policy is a more likely target for data intensive market intermediaries because they are deeply affected by data-localization. If they must localize data, then they must break up their operations into separate platforms, which would undermine efficiencies in the business model. And since digital platform intermediaries use data and algorithms to govern the exchange of goods and services in the economy, the primary concern is not privacy, but it is ensuring competition and digital rights. As Winseck put this across so eloquently in a recent conversation, we need policies that prevent digital actors from "thinking that they can construct the marketplace just because they own the network."

It may seem strange to combine media actors with intermediaries in this section, but it is essential to look at their data use practices in tandem. Data service companies such as ViaSense (http://locationgenius.com/) may be capable of creating a bridge between data for intermediation and data for persuasion. Also, it is somewhat artificial to separate persuasion from market intermediation; the two processes may be interlinked. This means that we

69 See: Jim Thatcher, David O'Sullivan and Dillon Mahmoudi (2017) "Data colonialism through accumulation by dispossession: New metaphors for daily data." *Environment and Planning D*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709498
70 http://www.cmcrp.org/the-growth-of-the-network-media-economy-in-canada-1984-2016/
71 This has been theorized convincingly in Nick Srnicek (2017) Platform Capitalism, Polity Press.

need to consider the policy overlaps between intellectual property, competition, innovation and privacy (or other data rights). These different policy areas should not be considered in isolation from each other.

In addition, we need to be aware of the fact that there is a power structure to the platform economy. While smaller platform companies may not leverage their data for anti-competitive practices, they make use of the services of larger platforms in ways that reinforce the market position and political and economic power of those platforms. This is as when a small platform like UrbanShare in Vancouver makes use of Facebook or Google to validate new users.

4.3 Purpose, Scale and Reach

Given that novel business practices can be adopted throughout the economy, purpose, scale and reach are also important considerations in establishing new regulatory frameworks. Consider just the goods-sharing services active in the Vancouver area. They range from Village Vancouver and the Thingery, which support new forms of community economic development, to Urban Share and Quupe which are online marketplaces that help people capitalize on the unused capacity in their consumer goods. Purpose matters because it influences how initiatives collect, evaluate and leverage data.

Scale is essential to this discussion, because scale creates new or additional affordances for companies. The effects of scale will depend on a number of factors. Clearly there are network effects attached to the size of a platform enterprise (as discussed in section 1 above). Larger networks may be better positioned to achieve market dominance, which would give them special kinds of influence. But the value of a data set is not necessarily proportional to its size. And small companies are just as likely to engage in third party authentication as larger ones, or work with credit card companies or cloud platforms. This means that their data footprint will be much larger than the number of people their client base might suggest.

The same set of considerations also applies to reach, particularly in reference to data localization. Larger companies will often reach across regulatory jurisdictions, however they are also in a better position to adjust their practices to meet local regulatory demands. Smaller companies are just as likely to work with third party service suppliers located in other markets, making data localization a significant issue for them. Very local companies, however, may be doing everything in house, which would make them fly under the radar of scale or reach issues. Clearly this set of considerations is ripe for empirical investigation.

4.4 Types of Regulation

A final consideration concerns the enactment of data regulations for the platform economy. Are data-intensive platform-based activities best regulated by a government authority, through industry self-regulation, or some other approach? The current approach in Canada favors industry self-regulation overseen by a government watchdog within a particular set of legal parameters. For example, Canada's Federal Privacy Commissioner, Daniel Therrien, can investigate privacy concerns that fall within the ambit of PIPEDA, and he can recommend criminal investigations. But he has no powers of enforcement.

A similar approach seems to be taking shape with regards to the data-intensive activities of platform businesses. According to Grossman (2015; also Hazenberg & Zwitter 2017) platform data could be regulated through data audits, mandated open access to one's own data, protections for data pooling efforts, and the like. However, this is a major challenge since most private enterprises eschew data transparency, given that data and algorithms are

central to their competitive advantage (Schiller, 2007). Workarounds to this problem are emerging. Several Canadian experts have suggested that companies could be required to inform clients about the scope and intent of their algorithmic practices, without revealing the contents of their codes. Regular data audits by government-approved third party practitioners could certify compliance with federal legal frameworks. Audits would then provide the basis for oversight, and if necessary, disciplinary measures.

However, most Canadian digital rights watchdogs would likely decry this approach. They have been dissatisfied with the limited powers of the Privacy Commissioner, and feel that the case law solution puts too heavy a burden on public 'Davids' to pursue private sector 'Goliaths' in court. Instead, they would favor greater enforcement powers plus regulations that empower citizens and consumers to access, share and audit private data themselves.

Appendix

Table of Key Arguments Debated by the "Personal Information" Policy Community in Canada

Methodology note

The following table summarizes the main arguments observed in two parliamentary reviews of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) in 2012 and 2017 respectively, and in newspaper articles about PIPEDA published in The Globe and Mail, Ottawa Citizen and National Post from 2012 to 2018. Specifically, the sample for the content analysis included: 1) the report produced by the House of Commons Standing Committee on Access to Information, Privacy and Ethics in April 2013 about the review of PIPEDA in 2012[72], 2) the official transcriptions of the meetings held during the second parliamentary review of PIPEDA in 2017 as delivered by the House of Commons website[73], and 3) Sixty two newspaper articles – 23 from The Globe and Mail, 19 from Ottawa Citizen and 20 from National Post – retrieved from the ProQuest Canadian Newsstream database through a search of the keyword 'PIPEDA'.[74]

Arguments	Actors
1.a) Big wave: PIPEDA is "a good law that meets the demands of industry and privacy rights, and facilitates self-regulation.[75]"	Private sector and industry associations
1.b) Big wave: PIPEDA needs to be legislatively revised and "modernized[76]" –arguments range from "making tweaks to PIPEDA, to wholesale reconsideration of the law[77]", with suggestions moving "from recognizing how the privacy landscape has changed and Canada's need to adapt to these changes through specific, privacy-related reforms, to larger reviews of a wider spectrum of data and consumer protection laws.[78]"	Public interest groups; academia; Privacy Commissioners
Little wave: The Office of the Privacy Commissioner (OPC) should have stronger enforcement powers – PIPEDA "has no teeth[79]"; "compliance by organizations remains problematic, largely because non-compliance carries minimal risk.[80]" Specifically, the OPC should be legislatively empowered to designate transparency reporting obligations and to ensure compliance with PIPEDA's accountability and openness principles.	Public interest groups academia; Privacy Commissioners

72 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. Retrieved from http://www.ourcommons.ca/DocumentViewer/en/41-1/ETHI/report-5

73 Official transcriptions of the meetings held in the House of Commons Standing Committee on Access to Information, Privacy and Ethics in 2017 retrieved from http://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=9213226

74 Newspaper articles were retrieved from the ProQuest Canadian Newsstream database through search of the keyword "PIPEDA".

75 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.31.

76 Testimony by Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada) House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 46. February 16, 2017. pp.2-3.

77 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.31.

78 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013 p.33.

79 Canada's privacy watchdog seeks stronger enforcement powers Krashinsky Robertson, Susan . The Globe and Mail; Toronto, Ont. [Toronto, Ont] 22 Sep 2017: A.1.

80 Testimony by Mr. Dennis Hogarth (Vice-President, Consumers Council of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 61. Tuesday, May 16, 2017. p.3.

Little wave: Accountability frameworks based on self-regulated industry standards and codes of conduct is preferable over legislated obligations.	Private sector and industry associations
Little wave: There is no need for stronger enforcement powers of the Privacy Commissioner at this time –"the current ombudsman model is best suited to the current principles-based framework[81]"; "additional enforcement powers for the OPC are not required at this time. Enhanced enforcement powers were provided… as recently as 2015 through the Digital Privacy Act.[82]"	Private sector and industry associations; law firms representatives
Little wave: The Digital Privacy Act is "carte blanche for companies to share Canadians' personal information with big media companies that are trying to crack down on copyright infringement.[83]"	Public interest groups; academia
Little wave: Regulatory bodies should establish "guidelines[84]" that assist businesses in the development of industry standards and practices that fully comply with PIPEDA.	House of Commons Committee on Access to Information, Privacy and Ethics
Little wave: PIPEDA's consent-based framework continues to be adequate –it is "a legally viable and practical means of authority under PIPEDA for organizations to collect, use, and disclose personal information in today's data environment[85]".	Private sector and industry associations
Little wave: Data collection "benefits consumers and businesses alike.[86]" Some of its derived provisions such as targeted advertising "can reduce the time consumers spend looking for products by focusing on the things of most interest to them[87]", while data collection can become a form of revenue and competitive advantage for companies.	Private sector and industry associations; The Globe and Mail open editorialist
Little wave: Current businesses and organizational practices for obtaining consent do not ensure that individuals are giving meaningful or valid consent when allowing companies to collect, use or disclose their personal information.	Public interest groups; academia; Privacy Commissioners
Little wave: Companies should improve transparency in their data collection, use, and disclosure practices and in "algorithmic decision-making"[88] processes, since "under PIPEDA, transparency is at the heart of the consent-based data protection scheme.[89]"	Public interest groups; academia; Privacy Commissioners
Little wave: Data anonymization offers an effective solution to	Private sector and industry associations;

81 Testimony by Mr. Robert Ghiz (President and Chief Executive Officer, Canadian Wireless Telecommunications Association). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 60. Thursday, May 11, 2017. p.4.

82 Testimony by Mr. Robert Watson (President and Chief Executive Officer, Information Technology Association of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 61. Tuesday, May 16, 2017. p.2.

83 Tories' digital bill raises fears over citizens' privacy; Freer Corporate Hand Ling, Justin. National Post ; Don Mills, Ont. [Don Mills, Ont]14 Apr 2014: A.5.

84 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. p.5.

85 Testimony by Mr. Adam Kardash (Partner, Privacy and Data Management, Osler, Hoskin and Harcourt LLP, Interactive Advertising Bureau of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 62. May 30, 2017. p.5.

86 Testimony by Mr. Jason McLinton (Vice-President, Grocery Division and Regulatory Affairs, Retail Council of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 63. June 1st, 2017. p.5.

87 Testimony by Mr. Jason McLinton (Vice-President, Grocery Division and Regulatory Affairs, Retail Council of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 63. June 1st, 2017. p.5.

88 Testimony by Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.4.

89 Testimony by Prof. Teresa Scassa (Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.3.

current consent issues with regards to personal information –"organizations now engage in a practice referred to as de-identification or anonymization or obfuscation (...) it protects individuals because the data can be rendered non-identifiable.[90]"	academia
Little wave: Consent provisions, especially express consent requirements, should move to a risk assessment-based model "where organizations are given more freedom but also more responsibilities over consumer data.[91]"	Private sector and industry associations; academia
Little wave: The move to a risk assessment-based model, or a more implied consent framework, "should be resisted[92]" –"such a framework would effectively amount to open season on individual data[93]".	Public interest groups
Little wave: Profiling is a worrisome by-product of big data analytics with implications for human rights, especially discrimination –"it can be used to characterize individuals as unworthy of special discounts or promotional prices, unsuitable for credit or insurance, uninteresting as a market for particular kinds of products and services.[94]"	Public interest groups; academia; Privacy Commissioners
Little wave: Canada should modernize PIPEDA in terms of implementing de-indexing rights, or the so-called 'right to be forgotten', especially for children and youth.	Public interest groups; privacy commissioner
Little wave: There a high risk on that a right-to-be-forgotten would infringe on freedom-of-expression rights.	Private sector associations, public interest groups; news organizations; academia
Little wave: Businesses should not have to strike the balance between an individual's privacy and freedom of expression –"these decisions are best left to the courts.[95]"	Private sector and industry associations; public interest groups.
2.a) Big wave: Canada should consider modernizing its privacy laws vis-à-vis the new European Union General Data Protection Regulation (GDPR), mostly to maintain Canada's status as an adequately protected jurisdiction for harbouring European data.	Privacy Commissioners, some public sector organizations, "industry observers[96]"
2.b) Big wave: Making legislative changes in PIPEDA vis-à-vis the new EU GDPR would be "premature[97]" –"a more precise view may be revealed going forward as we have more experience with the GDPR and its transborder adequacy review process.[98]"	Private sector representatives and industry associations

90 Testimony by Mr. Adam Kardash (Partner, Privacy and Data Management, Osler, Hoskin and Harcourt LLP, Interactive Advertising Bureau of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 62. May 30, 2017. p.7.

91 Testimony by Mr. Wally Hill (Vice-President, Government and Consumer Affairs, Canadian Marketing Association) House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 60. May 11, 2017. p.4.

92 Testimony by John Lawford (Executive Director and General Counsel, Public Interest Advocacy Centre). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 46. February 14, 2017. p.3.

93 Testimony by Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 49. February 23, 2017. p.3.

94 "Privacy and Social Media in the Age of Big Data". House of Commons Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. April 2013. pp.9-10.

95 Testimony by Mr. Robert Watson (President and Chief Executive Officer, Information Technology Association of Canada). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 61. Tuesday, May 16, 2017. p.2.

96 Calls grow for Canada to modernize privacy laws. Krashinsky Robertson, Susan. The Globe and Mail; Toronto, Ont. [Toronto, Ont]24 July 2017: B.1.

97 Testimony by David Young (Principal, David Young Law, As an Individual). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 54. April 4, 2017. p.2.

98 Testimony by David Young (Principal, David Young Law, As an Individual). House of Commons Canada. Standing Committee on Access to Information, Privacy and Ethics. Meeting Number 54. April 4, 2017. p.2.

3) Big wave: Data localization and cloud-computing creates concerns vis-à-vis the problems of holding jurisdictional control over private data of Canadians stored outside the country.	Public interest groups, academia, lawyers