

PROFITS OVER PRIVACY

PROFITS OVER PRIVACY: INVESTIGATING THE UNDER-REGULATED BUSINESS
PRACTICES OF THE GLOBAL DATA BROKERAGE INDUSTRY IN CANADA

By MACKENZIE PORTER, B.A, M.A

A Thesis Submitted to the School of Graduate Studies in Partial Fulfilment of the Requirements
for the Degree Doctorate of Philosophy

McMaster University © Copyright by Mackenzie Porter, September 2025

McMaster University, DOCTOR OF PHILOSOPHY (September 2025) Hamilton, Ontario
(Political Science)

TITLE: Profits Over Privacy: Investigating the Unregulated Business Practices of the Global
Data Brokerage Industry in Canada

AUTHOR: Mackenzie Porter, B.A (Queen's University), M.A (McMaster University)

SUPERVISOR: Professor Tony Porter

NUMBER OF PAGES xi, 127

LAY ABSTRACT

This dissertation sheds light on the global data broker industry and the ability of these firms to collect, buy, lease and/or sell Canadian personal information despite federal and provincial privacy laws. To explain the under-regulation of this industry, this dissertation identifies ways in which data brokers in this industry can use their power as businesses to shape, redirect or weaken privacy laws and regulations. However, this dissertation concludes that the under-regulation is due to a capitalist system that privileges commercial interests and the Government of Canada's limited knowledge of this industry.

To help consumers better understand this industry, the firms that comprise it and their business practices, this dissertation offers a unique categorization of data brokers and a list of data brokers that are operating in Canada. To better protect personal information, gaps in Canadian privacy laws are identified and a new approach for regulating data brokers is presented.

ABSTRACT

This dissertation contends that in pursuit of profits, Canada's privacy regime relies on quasi-self-regulation, non-prescriptive principles, and weak limitations on the collection, use, and disclosure of personal information—all of which permits and encourages the monetization of personal information by data brokers. As the government seeks to promote innovation and economic growth, commercial interests have been placed ahead of consumer privacy. The prioritization of profits over privacy, coupled with the Canadian Government's limited knowledge of data brokers, exacerbates the insufficient regulation of data brokers in Canada and minimizes the need for these firms to exercise their business power to advance their interests.

To advance this argument, this dissertation establishes a unique theoretical framework that lays the foundation to examine and explain the monetization of Canadian personal information by data brokers. Additionally, this dissertation employs a qualitative methodological approach that combines elite interviews, House Standing Committee testimony and an analysis of lobbying data.

This dissertation makes four key contributions to knowledge. First, by focusing on data brokers in Canada, this dissertation expands the literature on privacy, Big Data, and business power to an issue area and country that have received inadequate scholarly attention. With the novel digital age data broker typology and a Data Brokers in Canada List, this dissertation has provided empirical insights into an industry that is notoriously opaque. Second, it identifies three features of Canada's privacy regime that enable traditional and digital age data brokers to monetize personal information. Third, this thesis identifies five avenues of influence through which data brokers can, but largely do not, exercise their business power. Together, these avenues were utilized to diagnose a very weak degree of regulatory capture by data brokers. Lastly, this dissertation contributes to the understanding of regulation as a tool to mitigate harms and to promote innovation and highlights how capture theory inadvertently excludes implicit forms of capture that are still hazardous.

ACKNOWLEDGEMENTS

First and foremost, I am deeply grateful to my supervisor, Dr. Tony Porter, whose guidance and mentorship were instrumental in shaping this project. Without your intellectual curiosity, unwavering support and commitment to my academic development, completing this dissertation would not have been possible. Working with you on this and many other projects throughout my M.A. and PhD has been an invaluable experience and a profound privilege. Thank you.

Second, I would like to thank my dissertation committee: Dr. Sara Bannerman and Dr. Cliff van der Linden. Your insightful critiques, thoughtful questions, and valuable feedback pushed me to refine my research and strengthen my arguments. Your expertise was instrumental in shaping this work. I would also like to thank Dr. Teresa Scassa from the University of Ottawa for her role as the external examiner and for attending my defence in person; it truly made it a memorable experience.

Thanks are also due to Manuella Dozzi for her never-ending kindness and continuous guidance over the years, the Department of Political Science at McMaster University and to all the participants I interviewed to complete this project.

I owe an enormous debt of gratitude to my mother, Alison, and sister, Meagan, for all their support over the course of my B.A., M.A., and PhD. Your unwavering belief in my potential and endless encouragement through every stage of this journey were invaluable. I also want to acknowledge my late father, Dennis. Although he is no longer with us, his work ethic, determination, and relentless pursuit of excellence have been a constant source of motivation throughout this journey. This dissertation is dedicated to him.

Finally, to my partner, Adam, thank you for your resolute patience, support, and understanding. Words cannot describe how grateful I am for your commitment to my academic career and for your tireless efforts to make life outside of graduate school as stress-free and enjoyable as possible.

Table of Contents

Chapter 1: Introduction	1
Chapter 2: Literature Review	5
2.1: Privacy	5
2.2: Big Data and Data Brokers	9
2.3: Literature on the Role of Private Actors	13
Chapter 3: Theory and Methods	18
3.1 Theoretical Framework	18
3.2: Methodological Approach	28
Chapter 4: Monetizing Consumer Data: The Firms and Business Practices of the Data Broker Industry	31
4.1: Data Brokers and the Data They Sell.....	32
4.2: Digital Age Data Brokers: A New Typology	37
4.3: The Global Data Broker Industry in Canada	41
Chapter 5: Privacy Protections in Canada: A Perilous Paradox	47
Introduction.....	47
5.1 Canada's Patchwork Privacy Regime	48
5.2: The Discretionary and Interpretative Landscape of Canadian Privacy Law	53
5.3: Compliance and Enforcement: The Fate of a Powerless Regulator	59
Chapter 6: The Interests and Influence of the Global Data Broker Industry	66
Introduction.....	66
6.1: Justifying Data Monetization with Economics Assumptions	67
6.2: Don't Poke the Bear: Data Broker Lobbying in Canada and the United States.....	71
6.3: Additional Avenues of Influence	78
Chapter 7: Conclusion.....	84
Introduction.....	84
7.1: Key Contributions and Answering the Research Questions.....	84
7.2: Responsive Regulation in Canada	88
7.3: Avenues for Future Research.....	90
Works Cited.....	94
Appendix A: The Data Brokers in Canada List.....	121

LIST OF FIGURES AND TABLES

Table 1: Six general types of cooperative arrangements.....	14 -15
Figure 1: The Enforcement Pyramid and The Enforcement Strategies Pyramid.....	25
Figure 2: Pyramid of Supports and Sanctions for Regulating Medicines.....	25
Figure 3: Connections between Theoretical Framework and Empirical Chapter.....	28
Table 2: Seven Types of Consumer Attributes.....	34
Image 1: Data Axle Data Dictionary.....	35
Table 3: Provincial Privacy Laws	50
Image 2: Orange Privacy Policy.....	56
Image 3: Rogers Privacy Policy.....	57
Table 4: Communication Reports Filed by Data Broker.....	72
Chart 1: Communication Reports Submitted by Data Brokers.....	73
Table 5: U.S. Data Brokers that Lobby.....	74
Chart 2: Data Broker Lobbying by Issue Area.....	75
Figure 4: Example Enforcement Pyramid.....	90
Appendix A: The Data Brokers in Canada List	121

LIST OF ABBREVIATIONS

AI – Artificial Intelligence
AIDA – *Artificial Intelligence and Data Act*
B2B – Business-to-Business
B2C – Business-to-Consumer
CASL – *Canada's Anti-Spam Legislation*
CDP – Customer Data Platform
CEO – Chief Executive Officer
CPPA – *Consumer Privacy Protection Act*
CPTPP – Comprehensive and Progressive Agreement on Trans-Pacific Partnership
CRA – Credit Reporting Agencies
CRM – Customer relationship management
CRTC – Canadian Radio-television and Telecommunications Commission
CUSMA – Canada-United States-Mexico Agreement
DAA – Digital Advertising Alliance
DAAC – Digital Advertising Alliance of Canada
DaaS – Data-as-a-Service
DAP – Data Activation Platform
DPIA – Data Privacy Impact Assessment
DPM – Data management platforms
DPOH – Designated Public Office Holders
DSP – Demand-Side-Platforms
EU – European Union
FIP – Fair Information Principles
FIPP – Fair Information Practice Principles
FTA – Free Trade Agreement
GDPR – General Data Protection Regulation
GPS – Global Positioning System
IAB – Interactive Advertising Bureau
ICE – Immigration and Customs Enforcement
INDU – House of Commons Standing Committee on Industry and Technology
IP – Internet Protocol
ISED – Innovation Science and Economic Development Canada
MAID – Mobile Advertising ID/Identifier
ML – Machine Learning
MP – Member of Parliament
NHL – National Hockey League
OCAP® – Ownership, Control, Access and Possession
OECD – Organization for Economic Cooperation and Development
OPC – Office of the Privacy Commissioner of Canada
PIA – Privacy Impact Assessment
PIPEDA – Personal Information Protection and Electronic Documents Act
PTA – Preferential Trade Agreement
RCMP – Royal Canadian Mounted Police
ROI – Return on Investment

SPC – Student Price Card

SSP – Supply-Side-Platforms

SWIFT – Society for Worldwide Interbank Financial Telecommunication

TNC – Transnational Corporation

UDHR – Universal Declaration of Human Rights

UN – United Nations

UNDRIP - United Nations Declaration on the Rights of Indigenous Peoples

U.S.– United States

USD – United States Dollar

WTO – World Trade Organization

DECLARATION OF ACADEMIC ACHIEVEMENT

The research and findings presented in this dissertation are the sole and original work of the author. Throughout the project, there was no collaboration with colleagues or other contributors. Thus, the contents of this dissertation, including any mistakes are solely those of the author.

Chapter 1: Introduction

Social media platforms, smart phones, television, watches, homes, speakers and appliances, health and fitness tracking apps, online shopping, streaming services and loyalty programs have a myriad of social, psychological, physical and financial benefits for individuals and communities. For example, social media platforms help connect and build communities, smartphones provide real time navigation while loyalty programs can offer rewards points redeemable for savings. Running in tandem but in the shadow of these benefits is the monetization of the personal information individuals must disclose to use these technologies, apps and/or services.

Personal information or data “means any information relating to an identified or identifiable individual (data subject)” (OECD 2002a, p. 13). This can include age, financial information, marital status, education and medical history, nationality and race. To track a run with Strava, post a photo on Instagram or ask Google Home how to treat a burn, users must first set up an account or profile and may be required to share their personal information, such as name, email address, age and gender, to access the product or service. When using these digital consumer products and technologies, individuals knowingly or unknowingly disclose vast amounts of information regarding their demographics, preference, attitudes, behaviours, real-time locations and shopping habits (i.e., attributes). All this data can then be collected, linked to the user's account or profile and utilized to increase profits. Internally, firms can use this data to offer new products, personalized services or discounts to their customers. Externally, firms can generate new revenue streams by selling or sharing their customer's data with third parties looking to attract new customers, serve targeted advertisements, train AI algorithms or resell this data.

For firms, possessing a detailed knowledge of consumer behaviours can assist with targeting products and advertisements, lower advertising costs and providing personalized services (Acquisti 2014). The rise of this new logic of accumulation, also known as surveillance or information capitalism, aims to predict and modify human behaviour to produce revenue and market control (Zuboff 2015). Conversely, for individuals unprecedented amounts of personal information collected by e-commerce firms¹, platforms, smartphone applications, websites and wearables has resulted in a privacy crisis as consumers who have no control over how their data is used. Central to the growth of information capitalism and this privacy crisis is the global data broker industry.

Data brokers, which can also be referred to as information brokers, data providers, data aggregators, or consumer intelligence providers, are firms that harvest, collect, aggregate and monetize personal information. To do so, data brokers can sell static lists of consumer information, license access to a data product, or provide firms with additional data on their existing customers. Unlike the firms providing the digital consumer products and technologies discussed above, data brokers are not consumer facing. Instead, these firms operate in the shadows of the tech sector by utilizing highly technical and clandestine business practices to monetize personal information without attracting the attention of regulators, policymakers or the public. By tracking users' browsing habits with pixel tags, running surveys or questionnaires, scraping social media platforms, partnering

¹ E-commerce or electronic commerce refers to the buying and selling of goods or services using the internet. There are four types of ecommerce models, however, for this dissertation the focus will be primarily on B2C (Business to Consumer) and B2B (Business to Business) transactions.

with loyalty programs or purchasing data from retailers or other data brokers, the global data broker industry is not only surviving but thriving in the digital age. ThinkDataWorks (2025), a Toronto based ‘data catalogue provider’ (i.e., data broker) projects the global data monetization market will reach \$1.7 trillion by 2028 with an estimated 7-year compound annual growth rate of 17.5 percent. As the data-driven-economy and the global data broker industry continue to grow, consumers will have less control over their personal information.

For example, LexisNexis, one of the largest data brokers in the United States, has over 78 billion records from over 10,000 sources and uses 442 nonmedical attributes to predict patients’ health risks and costs (Allen 2018). With very limited knowledge on the specific information data brokers possess, individuals are unable to determine if their information is accurate or correct. The use of inaccurate data could result in an individual being denied health insurance. The pervasive collection of data to serve targeted advertisements and personalized products can also lead to psychological harms. In 2018 an American woman, Gillian Brockell, wrote an open letter to Facebook, Instagram, Twitter (now X) and Experian as she was being served parenting ads after learning her baby would be stillborn. In her letter, Brockell wrote “I know you knew I was pregnant. It’s my fault, I just couldn’t resist the hashtags - #30weekspregnant, #babybump...But didn’t you also see me googling ‘baby not moving’? Did you not see the three days of silence, uncommon for a high-frequency user like me? And then the announcement with keywords like ‘heartbroken’ and ‘problem’ and ‘stillborn’ and the two-hundred teardrop emoticons from my friends? Is that not something you could track?” (Brockell 2018).

In addition to harvesting and monetising the personal information and preferences of consumers from online sources, data collected from offline sources can be just as profitable. From marriage announcements in newspapers to census data to legal filings this offline data can be used to reduce costs and increase the accuracy of targeted advertising campaigns (Goldstone 2023). By combining off and online data, which brings offline data online, advertisers, retailers and data brokers can generate valuable and actionable insights into consumers at an individual, postal code and/or neighbourhood level. With loyalty and rewards programs being offered by grocery stores, gas stations and clothing retailers all companies are data companies. Factoring in the digital consumer products, for Jeff Chester, founder of the Center for Digital Democracy “Today, everyone is a data broker. Having the ability to reach someone online and target has become a core part of business” (in Booth 2024).

The vast amounts of off- and online personal information being harvested and monetized by firms across the data broker industry raises significant privacy concerns. There is little transparency around the ways in which data brokers collect, harvest or acquire personal information and from what sources. With vague privacy policies that rely on weak consent clauses and state ‘your personal information will be shared with third parties or ‘business partners’, i.e., data brokers, individuals have little to no knowledge on the entities with which their personal information will be shared. Without this knowledge individuals cannot give meaningful consent to the uses of their data. The pervasive, covert and highly technical ways in which data brokers obtain personal information further prevents individuals from understanding how their purchases, posts and web searches are being compiled and continuously monetized by data brokers. The weak consent clauses and information asymmetries prevent individuals from making informed decisions about protecting or

disclosing their data. After this data has been collected, individuals have minimal control over how it is used and re-used or if the data is correct and accurate.

Even with the highly invasive and widespread collection and monetization of personal information by data brokers, this industry has largely avoided scrutiny from legislators, regulators and the public. In both the absence and presence of statutory privacy protections data brokers have experienced minimal government intervention. In the United States there is no federal private sector privacy law to afford Americans with protections for how their personal information is collected, used and monetized. To fill this void, privacy statutes and regulations at the state level are being proposed and enacted. Conversely, in Canada there is a mix of national and sub-national privacy laws that aim to safeguard personal information when it used by firms. Across these various privacy laws there are a mix of privacy protections that afford individuals in certain jurisdictions with more control over and access to their personal information. Despite the presence of these national and sub-national statutes, data brokers continue to harvest, collect, and profit off personal information.

Focusing primarily on the global data broker industry in Canada, this dissertation seeks to explain and unpack the factors that contribute to the ongoing monetization of Canadian consumer data. Thus, the primary research question guiding this dissertation is as follows: why can data brokers purchase, sell, license and/or append the personal information of Canadians notwithstanding national and sub-national privacy statutes that call for limitations on the collection, use and disclosure of personal information? This dissertation poses and addresses two secondary questions. One, are data brokers, individually and/or collectively, exercising their business power through instrumental, structural and discursive channels to remain under-regulated? Two, is the business power and private interest influence of data brokers resulting in a strong or weak degree of regulatory capture?

This dissertation argues that, in pursuit of profits, innovation and economic growth Canada's privacy regime has and continues to rely on quasi-self-regulation, non-prescriptive principles and weak limitations on the collection, use and disclosure of personal information—all of which permits and encourages the monetization of personal information by data brokers. As the government seeks to reap the benefits of free market capitalism, commercial interests have been placed ahead of consumer privacy. The prioritization of profits over privacy coupled with the Canadian Government's limited knowledge of the data brokers industry further contributes to the insufficient regulation of data brokers in Canada and minimizes the need of these firms to exercise their business power to advance their interests.

1.2 Structure of Dissertation

This dissertation is organized into seven chapters. Following this introductory chapter, Chapter 2 introduces and reviews three bodies of literature that this dissertation contributes to and advances. By engaging with literature on privacy, Big Data and data brokers and the role of private actors, Chapter 2 establishes the foundation upon which the proceeding chapters build. Chapter 3 presents a unique combination of three theories, the economics of privacy, capture theory and responsive regulation, that are employed to inform this dissertation's examination of the data broker industry in Canada and theoretical contributions. Additionally, Chapter 3 outlines the methodological approach utilized to guide the collection of data for the three empirical chapters.

Chapter 4 commences the empirical contributions of this dissertation by reviewing the firms that comprise the data broker industry, the types of data they collect and their business practices. This chapter differentiates between traditional data brokers, firms that buy and sell consumer data, and digital age data brokers, firms that monetize consumer beyond strictly buying a selling static list. In doing so, this chapter presents a unique six-category typology of digital age data brokers. Additionally, this chapter also identifies over 150 data brokers operating in Canada. The Data Brokers in Canada list can be found in Appendix A.

Chapter 5 focuses specifically on the features of Canada's privacy regime that fail to safeguard privacy and enable data brokers, both traditional and digital age data brokering, to profit from personal information. This chapter commences by outlining and discussing the statutes that comprise Canada's privacy regime and associated the challenges firms face in navigating this complex patchwork of laws. The chapter then proceeds to discuss the quasi-self-regulatory elements of the federal privacy statutes that afford firms a great deal of discretion in how they use and protect personal information. Lastly, the chapter examines the weak enforcement power of Canada's privacy regulator, The Office of the Privacy Commissioner. Together, these three sections highlight how Canada's privacy laws produce a regime that promotes profits and innovation the expense of privacy.

Chapter 6 presents and examines two primary (economic assumptions and lobbying) and three secondary (House Committee testimony, industry associations and Government partnerships) avenues of influence through which data brokers can advance their individual and collective interest. In doing so, this chapter works to determine if data brokers operating in Canada utilize these avenues to remain unregulated. Chapter 6 also examines the formal lobbying activities of both Canadian and American data brokers to determine if there are consistencies industry wide. Through the analysis of these avenues of influence this chapter diagnosis the degree of regulatory capture in Canada by the data broker industry.

A concluding chapter reiterates the key findings presented in this dissertation that were utilized to answer the primary and secondary research questions as well as support the central argument. Following this overview, the chapter proceeds by highlighting the ways in which responsive regulation can be applied to address the global data broker industry and its operation in Canada given the existing privacy regime. Lastly, this chapter identifies three areas for future research.

Chapter 2: Literature Review

Introduction

For this dissertation, I will be taking an interdisciplinary approach, drawing on literatures across the fields of political science, economics, and legal studies. More specifically, this dissertation seeks to employ, bridge and expand on three bodies of literature. These include the literature on privacy in the fields of politics, economics and law, the literature on Big Data and data brokers, and lastly, political economy literature on business power and private interest influence. This chapter will synthesize the key findings, themes, and debates across these three bodies of literature. In doing so, this chapter seeks to identify gaps across the literature that this dissertation will work to fill over the three empirical chapters.

The chapter is organized as follows. Section 2.1 engages with the literature on privacy by tracing the origins of the right to privacy and how this notion shapes statutes, guidelines and expectations for individual and organizational privacy, yet fails to provide any substantive privacy protections for consumers in era of Big Data. Section 2.2 overviews the literature on Big Data that this dissertation is founded on and seeks to advance. This section acknowledges the small yet growing body of literature on Big Data and data brokers as well as some relevant debates such as the value of Big Data and the role of technology in shaping society. Lastly, since there is minimal government regulation in the data broker industry, the political economy literature on the role of privacy actors in Section 2.3 will be utilized to provide explanations for how actors in this industry exert their power and authority to self-regulate.

With this chapter, I seek to highlight that the majority of the literature on privacy, Big Data and the role of private actors is centered around the United States. Additionally, despite a growing interest in privacy in the information age, there remains a substantial lack of literature on data brokers. Therefore, one objective of this dissertation is to fill these gaps by focusing on the privacy violating practices of data brokers in Canada.

2.1: Privacy

2.1.1: The Right to Privacy

To safeguard against intrusions by public institutions and private actors, individuals in the West have been granted numerous forms of privacy protection. Protecting privacy is a fundamental and widely accepted value in liberal democratic societies as it affords individuals autonomy, solidity, intimacy, and anonymity, all of which underpin the concept of democracy based on individual choice (Bennett and Raab 2003; K. Laudon 1996; Westin 1967). However, privacy is an elusive concept with no generally accepted definition (Acquisti, Taylor, and Wagman 2016a; Bennett 1991; Phelps, Nowak, and Ferrell 2000; R. A. Posner 1978).

Western scholarship on privacy has been and continues to be heavily influenced by American legal literature. In particular, the modern conception of privacy and the notion of a right to privacy originated in Warren and Brandeis' "The Right to Privacy" published in an 1890 issue of the *Harvard Law Review*. Warren and Brandeis were the first to systematically describe a legal right to privacy, defining it as a right to protect one's "inviolable personality" from intrusion or unwanted revelation (DeVries 2003). In their article, Warren and Brandeis further articulate their conception of a right to privacy as "... the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone" (Warren and Brandeis

1890, p. 205). Privacy as the right to be let alone is commonly attributed to Warren and Brandeis, however, the idea of a right to be let alone was first discussed by Justice Thomas Cooley in 1880 as a protection from intrusion under tort law (Cooley 1880). Privacy torts are a substantive legal regime that is effective when applied in situations involving specific and traceable individualized harms but is limited when dealing with small and probabilistic harms (Strandburg 2014).

Beyond U.S. tort law, the notion of a right to be let alone has been discussed as a constitutional right. However, the United States Constitution does not include privacy as a fundamental right (Laudon 1996a; Rubinfeld 1989). In several instances lawyers and the U.S. Supreme Court have found privacy protections in the “penumbras” of the first, fourth, fifth, ninth and fourteenth amendments, however these rights have only been extended to couples purchasing contraceptives (*Griswold v. Connecticut*, 1965) and the sexual conduct of same sex couples (*Lawrence v. Texas*, 2003) (Breckenridge 1970; Laudon 1996; O’Brien 1979; Rubinfeld 1989).

In 1967, the concept of privacy and the field of privacy laws were transformed again with the release of Alan Westin’s book *Privacy and Freedom*. For Westin (1967 p.7), privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”. Following in the steps of Westin, many other scholars also recognized privacy as a group-level concept whereby groups, through the development and application of norms or rules, regulate what information is released to which others (Laufer and Wolfe 1977; Margulis 1977; Westin 1967). Around this time, the widespread computerization of legal, financial, medical, and other personal records catapulted information privacy and concerns regarding the desire and ability to control how much personal information we reveal to others to the forefront of scholarly debates (Bélanger and Crossler 2011; Fox 2013).

In the 1970s the U.S. Department of Health, Education and Welfare (hereby: HEW) established a committee to address the growth of automated data systems that contained personal information about individuals (Borgesius, Gray, and van Eechoud 2015; DeVries 2003; Gellman 2014). The *Records, Computers and the Rights of Citizens* report published by the committee contained a Code of Fair Information Practices which was the first explicit reference to “fair information practices” or FIPs (OECD 1980). The privacy concerns that initiated the HEW’s committee also led governments in other OECD countries, including Canada, the Netherlands and France, to create task forces, commissions, and committees to study similar issues (OECD 1980). In 1980 the OECD proposed and adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* which included eight principles that generally proposed rights and remedies for data subjects (Gellman 2014). In addition to recognizing that member countries have a common interest in protecting privacy, the guidelines also recognized that transborder data flows contribute to economic and social development and that domestic privacy legislation may hinder transborder data flows (OECD 1980). Since the OECD principles have been incorporated into the information privacy statutes of most advanced industrial states (Bennett and Raab 2003), many of these statutes are thus built around the premise that protecting privacy can be balanced with promoting the free flow of information. However, as will be discussed, these two objectives cannot be pursued simultaneously

In addition to individual and group privacy, the rapid computerization of records also initiated a discussion on the privacy rights of organizations i.e. firms. On one side of the debate there

are discussions regarding the privacy rights afforded to organizations and on the other, there are discussion on the privacy practices of organizations. For scholars such as Westin, “privacy is thus not a luxury for organizational life, it’s a vital lubricant of the organizational system in free societies” (1967). Privacy is a necessary element for the protection of organizational autonomy, gathering of information, perpetration of positions, internal decision making and conducting business (Savoie et al. 2020; Westin 1967).

For other scholars, the focus is on the privacy practices of organizations that utilize the personal information (Cespedes and Smith 1993; Culnan and Williams 2009; Malhotra, Kim, and Agarwal 2004; Phelps, Nowak, and Ferrell 2000; Smith, Milberg, and Burke 1996). In this camp, scholars seek to examine consumers’ concerns with the business and privacy practices of firms. More recently, the focus has shifted to e-commerce firms and platforms. Known as the Privacy Paradox or the attitude-behaviour dichotomy, scholars have revealed discrepancies between user attitude and their actual behavior towards protecting their privacy online (Barth and de Jong 2017). Whether it is attributed to convenience, lack of awareness or decision-making biases, users have a tendency towards privacy-compromising behaviour online despite their positive attitude towards privacy-protection behavior (Acquisti and Grossklags 2005; Aguirre et al. 2015; Barth and de Jong 2017; Martin 2020; Palmatier and Martin 2019). The debates and discussions by scholars on both sides of organizational privacy will be influential to the enduring contribution to the larger body of privacy literature that this dissertation seeks to make.

A substantive portion of the literature on privacy, especially information privacy, is centered around the privacy of individuals, groups, or organizations in the U.S. Despite the differences in the American and Canadian legal and political systems, these American legal scholars have greatly influenced how privacy is viewed, protected and violated in Canada. One crucial area in which American literature and events have shaped privacy in Canada is the debate between privacy and national security in the post-Snowden era (Austin 2015; Geist 2015; Vedaschi 2018). Despite the significance of the privacy-security paradox, especially with the use of modern networked digital technologies as tools for surveillance (Office of the High Commissioner for Human Rights 2022), the invasions of privacy carried out by government institutions in the name of national security are beyond the scope of this project’s focus on private sector actors.

With newly emerging technologies, privacy in a high-tech world has taken on many new dimensions (Savoie et al. 2020). The rise of machine learning and Big Data analytics also reignited and reinvented the idea of group privacy discussed by Alan Westin in the late 1960s. With Big Data and machine learning, new information can be inferred about pre-existing groups, non-apparent groups can be identified in pre-defined parameters or new groups can be identified using new analytical approaches, (Kammourieh et al., 2017), all of which can assist firms in better identifying their target audiences. Since data is no longer about one specific individual, but is rather about large and undefined groups, the focus on the individual and personal data is too narrow and should be supplemented by an interpretation of privacy at the group level (Taylor et al., 2017). Thus, the idea of group privacy implies that “groups can have a form of privacy that amounts to more than the mere fact of being sets of individuals each of whom has individual privacy” (Loi & Christen, 2020, p. 209).

Big Data and machine learning are only two examples of technological advancements in the digital age that are highly profitable to firms but are exacerbating privacy violations for both groups

and individuals. With the research published by scholars studying privacy invasions arising from facial recognition, patient data, smart cities, and Internet carriers (see Bannerman and Orasch, 2020; Lane et al., 2014; Obar, 2022; Slane, 2021; Spithoff et al., 2022) it becomes increasingly clear that public and private sector actors can profit or benefit from surveillance technologies that track the Internet searches, purchases, and locations of both individuals and groups.

2.1.2: Digital Trade and Cross-Border Data Transfers

With the digitalisation of the economy, the intersection of digital trade and privacy has emerged as a major topic of discussion. At the heart of these discussions and the data-driven economy is the free flow of information across borders (Laidlaw 2021). The data-driven economy refers to the collection, aggregation, organization, analysis, exchange, and exploitation of digital information that is then used to innovate, produce, operate, and sell responsive machines, goods, and services (Shaffer 2021). Thus, to have a thriving data economy, data must cross borders freely (Burri 2017). With the internet and transborder data flows becoming important channels of trade, states are looking to implement and use digital trade policies to meet economic objectives (Azmeah et al., 2020). Despite no agreed-upon definition of digital trade, “there is a growing consensus that it encompasses digitally enabled transactions in trade in goods and services which can be either digitally or physically delivered and which involve consumers, firms, and governments” (González and Jouanjean 2017 p.2).

Even with an economic era marked by the datafication of all social, political and economic activity (Ciuriak 2018), there are almost no international rules governing how data is traded.² Since 1995, the World Trade Organization (WTO) has been the primary multilateral forum for negotiating and governing international trade. However, Weber (2010) argues that WTO laws do not provide an adequate legal framework to address digital trade rules. Recognizing the implications of digitalization for trade in 1998, WTO members agreed to a moratorium on imposing customs duties on electronic transmissions that is still in place today (Burri and Polanco 2020; Leblond 2022). Since then, existing WTO rules such as the General Agreement on Trade in Services (GATS) have been applied to digital trade, products and services. How a transaction is delivered and what type of product is being transacted determines which agreement it faces since trade policy commitments and rules differ for goods (GATT) and services (GATS) (González and Jouanjean 2017).

The GATS Council on Services has determined that much of e-commerce falls within the GATS’ scope, GATS obligations cover electronic service delivery and that GATS applies even as technology changes a service’s delivery (Aaronson and Leblond 2018). However, unresolved issues include classifying and defining chat applications such as WhatsApp, virtual meeting services such as Zoom and search engines such as Google that are not explicitly named under the GATS Provisional Central Product Classification (Peng 2023). The GATS Council on Services has also noted that governments are free to regulate services so long as there are no unnecessary barriers to trade (Aaronson and Leblond 2018). With the GATS containing few disciplines on domestic regulation, the key question is when and under what conditions can legitimate policy objectives trump digital trade interests? (Peng 2023)

² Minor exceptions include EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework.

With the WTO failing to address the new realities of digital trade, the 1998 moratorium has been regularly renewed and incorporated into bilateral or plurilateral free trade agreements (FTAs) such as Canada's Comprehensive Economic and Trade Agreement (CETA) with the EU and the Canada-United States-Mexico Agreement (CUSMA) (Leblond 2022). More specifically, states have begun including provisions on e-commerce, cross-border data flows, and privacy protections in their bilateral and plurilateral FTAs or preferential trade agreements (PTAs) (Elsig and Klotz 2021; Velli 2019). Scholars have explored the inclusion and evolution of digital trade provisions in trade agreements across and between countries in Asia (Rahman and Rahman 2022), the European Union (EU) (Sauvé and Soprana 2020), Latin America (Aguerre 2019), and the U.S. (Gao 2018). For many scholars, privacy protections, such as data localization are seen as barriers to trade and thereby reduce the gains from digital trade (Bauer and Lee-Makiyama 2014; Brehmer 2018; Meltzer 2019).

As digital trade expands, governments must simultaneously maximize the opportunities from data flows for trade and manage the impact of cross-border data flows on privacy and national security (Meltzer 2019; Suh and Roh 2022). For protecting data that crosses borders, there are four broad approaches. First, there is the absence of restrictions on the movement of data, second is ex-post accountability if the data is misused, third are conditions on data transfers via an adequacy determination and lastly, permitting data transfers on a case-by-case basis (Casalini and González 2019). For example, Australia permits data to be exported to jurisdictions with substantially similar privacy protections, the EU prioritizes data protection and prevents the export of data to countries with inadequate privacy laws, while the U.S. lacks federal privacy laws but is party to trade agreements that set a privacy floor (Aaronson 2020; Meltzer 2015). However, with firms, especially e-commerce firms, operating in different jurisdictions than their consumers, the enforceability of these privacy protection is diminished when firms transmit data to jurisdictions with less stringent laws to escape strict regulatory responsibilities (Bennett and Raab 2003).

2.2: Big Data and Data Brokers

Data can be collected or retrieved from billions of sensors in a wide range of devices including wearables, public and private databases, websites, and surveillance cameras (Constantiou and Kallinikos 2015). With these new technologies, Big Data has gone from minimal use in academia and industry in 2008 to a buzzword in business circles and popular media (Kitchin 2014). Conceptually, Big Data has no singular definition, because, according to Shoshana Zuboff "we continue to view it as a technological object, effect or capability" when it originates in the social (Zuboff 2015). For others such as Constantiou and Kallinikos (2015 p. 55), "big data is part and parcel of wider developments that concern contemporary patterns of living on and off the Web. These in turn are closely associated with the ways by which information is generated, made available or shared, and information-based services are produced and consumed." It is however, commonly agreed upon that data becomes Big on the dimensions of volume, velocity, variety (Kitchin 2014; Laborde 2020; McAfee and Brynjolfsson 2012).

In addition to the 3Vs, there are several other key characteristics of Big Data identified across the literature. These include Big Data as flexible, exhaustive in scope, fine-grained in resolution and relational in nature (Dodge and Kitchin, 2005; Mayer-Schönberger and Cukier, 2014; Warren and Marz, 2015). The Big Data trend has created an attitude toward collecting data for the sole purpose of collecting data resulting in most data acquisition scenarios assuming high-volume velocity variety with low-value data (Constantiou and Kallinikos 2015; Lyko, Nitzschke, and Ngomo 2016).

However, basing decisions, such as marketing strategies, on inaccurate data can have far-reaching negative consequences making it crucial for firms to collect accurate data (Cote 2022).

Growing alongside and with the technologies and raw data generated by the Big Data movement is the data broker industry. Data brokers are companies that “collect consumers’ personal information and resell or share that information with others” (Ramierz in Kim 2023, p. 2). Data brokers, can acquire Big Data by collecting information that is in plain view, acquiring data as a by-product of another activity or through the transfer of pre-existing information (Strandburg 2014). In terms of data that is in plain view data brokers harvest personal information online from two sources: public records such as arrests, mugshots, court decisions, and bankruptcy records; and user-generated content hosted on social media platforms and sites (Slane 2018). For the acquisition or transfer of data, this depends on the data brokers relationship with the consumer and other firms.

Using a variety of technologies and data acquisition methods data brokers collect and monetize personal information online via cookies, social media profiles and cellphone tracking and, offline through driving records, property deeds and marriage certificates (Crawford 2014; McClelland 2021; Zuboff 2015). However, validated offline data points are valuable, but only matter if they can be matched to online identifiers such as IP addresses, mobile signals, device IDs or location coordinates (Goldstone 2023). These modes of acquisition can be distinguished as first and second usages of personal information, where the former facilitates the firm’s interactions with customers and the latter occurs when firms share information with other firms, such as third parties (Varian 2009). Through these avenues of acquisition, all firms, from manufacturing to logistics to retail are data companies (Tarnoff 2018).

Not all data brokers harvest, collect, process and sell or share the same types of personal information. There are data brokers that exclusively focus on pharmaceutical, mental health and patient data (Kanwal and Walby 2024; Kim 2023; Spithoff et al. 2022a), educational data of both teachers and students (Amo et al. 2019; Arantes 2024; Simmons 2023) and the financial or credit data of consumers (Roderick 2016). The data collected and aggregated by these data brokers can be used for marketing purposes or fraud detection, sold to insurance and mortgage brokers or traded to other data brokers (Aïmeur et al. 2022; Stouffer 2023). In addition to these health, education and financial information data brokers there are also data brokers that specialise in selling business contact information, location data or personal information to other individuals (people search)(Latto 2020).

Through the collection and acquisition of these data, data brokers are intimately familiar with the personal information and lives of consumers but are poorly understood by many consumers themselves (Rostow 2017; Stouffer 2023). For example, an advertiser could target ‘children’s cereal buyers’ (relying on data collected and analyzed by third-party data providers) who live in Washington, D.C. (relying on data that a user has provided directly to Facebook or Twitter) (Rieke et al. 2016). In addition to algorithmically targeted advertising on social media, advertisers can also combine off and online data and use platforms such as Facebook to create ‘lookalike audiences’ to target ads to consumers that share similarities with their current customers (Burgess et al. 2024; Rieke et al. 2016). What has become evident through the small yet growing body of literature on data brokers is the fact that states have not taken an active role in protecting the privacy of citizens

when it comes to consumer data broker companies, especially in regulating third-party-data collection (Roderick 2014).

Typically, data brokers collect data without the knowledge or consent of the individuals involved nor do they inform the users of the implications and intended uses of the data being collected (Kanwal and Walby 2024). One notable example is Turnstyle Analytics placing sensors throughout Toronto businesses to gather signals from smartphones searching for open Wi-Fi networks so they could identify and track users across the city to then anonymize this data and sell it back to these businesses to help them better understand their customers (Crawford 2014). Not only did this process occur without the knowledge of the smartphone user, but an additional concern that arises within discussions on Big Data and data brokers is the ease in which anonymized or de-identified data can be reverse engineered (Bradford, Aboy, and Liddell 2020; Crawford 2014; Narayanan and Shmatikov 2010).

With the adoption of data-driven targeting techniques, the marketing and advertising industry has turned away from mass advertisements distributed indiscriminately to direct marketing campaigns that rely on consumer demographics, psychographics and buying habits (Gray 2019). The idea of segmenting consumers for marketing and advertising purposes is not a novel concept and in fact, has been around since the 1970s when Claritas developed *PRIZM* which defined groups of consumers based on demographics and behaviours (United States Senate Committee on Commerce, Science and Transportation 2013). Although segmenting consumers is still a prominent practice today, the tremendous increase in the volume of personal information available and the technological advances facilitating the storage and analysis of this information is propelling the data broker industry forward in ways never seen before (Rieke et al. 2016).

The collection and commodification of personal data through Big Data, AI and algorithms have been a foundational component of a new deeply intentional logic of accumulation that Shoshana Zuboff calls surveillance capitalism. Coined in 2014, surveillance capitalism is the “unilateral claiming of private human experience as free raw material for translation into behavioural data. These data are then computed and packaged as prediction products and sold into behavioural futures markets — business customers with a commercial interest in knowing what we will do now, soon, and later” (Zuboff in Laidler, 2019). These accumulation techniques represent a new form of surveillance that is less to do with a centralized state-led panopticon targeting individuals and is more concerned with promoting various data marketplaces that trade the valuable and dominant asset of personal data (Andrew and Baker 2021; Therrien 2021; Zuboff 2015).

For states, firms and individuals, Big Data can be seen as both harmful and beneficial to society as advances in data acquisition and analytics can deteriorate fundamental values such as autonomy, while simultaneously adding to the stock of social and scientific knowledge (Barocas and Nissenbaum 2014; Strandburg 2014). These two divergent camps can be more specifically divided into techno-utopian and dystopian perspectives where the former praises the improvements algorithms have made for governance, decision making, and society and the latter addresses the negative effects of Big Data for power and control (Campbell-Verduyn, Goguen, and Porter 2017).

With an increasing amount of data produced daily and advancements in Big Data analytics, the speed in which large data sets can be processed is disrupting traditional business models

(Cavoukian, Stewart, and Dewitt 2012). For techno-utopian scholars, this acceleration is beneficial for marketing campaigns, engaging consumers, providing personalized services and addressing issues such as traffic congestion (Anshari et al. 2019; Arthur 2014; Bachechi, Po, and Rollo 2022; Chandra et al. 2022; Hofacker, Malthouse, and Sultan 2016). Conversely, techno-dystopians have highlighted the race and gender biases of algorithms, the rise of technosecurity and surveillance practices with Big Data, the effects of filter bubbles on democracy and manipulation through digital advertising (Anupam Chander 2017; Calo 2014; French and Monahan 2020; Heilweil 2020; Skinner 2020; Zittrain 2014; Zuboff 2015).

In addition to concerns about surveillance and biases, issues surrounding sharing or protecting personal data have emerged as crucial nexuses of economic and policy debate on Big Data (Acquisti, Taylor, and Wagman 2016a). For individuals and consumers, Big Data undermines the quality, accuracy and security of their personal information held by firms. An outright ban on the collection and use of data would however be disadvantageous for consumers, leading to increased costs, no personalized services and market inefficiencies (Posner 1978; Stigler 1980; Varian 2009). Privacy concerns have emerged alongside the advancement in Big Data collection, processing, and storage techniques, especially when anonymized datasets can be easily attacked and reconstructed (Cavoukian, Stewart, and Dewitt 2012; O’Leary 2015; Pence 2015; Yu 2016). The conflicting desires of firms and consumers on uses of personal information provides a unique opportunity for my dissertation to contribute to the literature on Big Data and privacy and fill a gap in the secondary usage of consumer data by data brokers, especially in Canada.

Stemming from the techno-utopian versus dystopian dichotomy, there is a secondary debate on technological determinism and the politics of technology that is central to the discussion on Big Data today. Technological determinism is the claim that technology causes or determines the structure of the rest of society and that technological developments take place outside society, independently of social, economic, and political forces (Wyatt 2008). Tools, instruments, and technologies are so worldly and influential that entire nations or millennia are classified and referred to using a single material artefact (i.e., the “stone” “iron” or “information” ages) (Arendt 1958; Mumford 1961; Wyatt 2008). The issue of technological determinism is that artefacts are often seen as neutral instruments when they do have political properties that embody forms of authority and subordination (de Vries 2017; Winner 1980). As seen in the work of the dystopian scholars discussed above, technology clearly has political properties and should thus be treated as political artefacts. However, with Big Data and autonomous algorithms, there are increasing complexities regarding the nature of these technologies and their relationship to society.

Autonomous technology is the claim that technology is not in human control, that it develops with a logic of its own, however, this is not to say that technology acts alone as human beings are involved (Feenberg 2006; Hallström 2022). The question that arises then is: do humans have the freedom to decide how autonomous technology will develop and be applied? (Feenberg 2006; Hallström 2022). Given the current roles of technology, I align this dissertation with the techno-dystopian perspective as data brokers and third parties are humans employing Big Data and algorithms to increase their capital and better their position in the market. Additionally, for consumers the harms and privacy violations arising from the harvesting and monetization of personal information by data brokers outweighs the benefits of personalized services and discounts. Using the economics of privacy theory, presented in Chapter 3, this dissertation seeks to highlight the hidden

costs and consequences of consumers disclosing their personal information to access ‘free’ products and services.

2.3: Literature on the Role of Private Actors

Across the field of GPE, scholars have investigated the complex linkages between political and economic activity, identified the sources and consequences of power and analyzed the distribution of absolute and relative gains from market activity (Cohen 2007; Gilpin 2001; Strange 1991). Central to both mainstream and critical GPE scholarship is the role of power and authority. While power and authority are closely related, they are not synonymous.

To advance their business interests and shape policies, firms can exercise their private influence and power through various channels. For Doris Fuchs, the political power of businesses is three-dimensional. First, instrumental power is based on the idea of individual voluntary action and focuses on the direct influence of an actor on another actor (Fuchs 2007). Lobbying is one of the primary political activities through which businesses exercise their instrumental power to influence formal decision making processes (Fuchs 2007). The second dimension of business power is structural power. Structural power emphasizes the input side of policymaking and it is exercised by firms through agenda and rule setting (Fuchs 2007). Firms can exercise agenda-setting power through their ability to reward and punish governments for their policy choices by moving capital and jobs (Fuchs 2007). Lastly, firms can exercise discursive power by shaping ideas, norms, identities and perceptions (Fuchs 2007). The promotion of privatization, for example is a reflection of firms exercising discursive power (Fuchs 2007). These three avenues of business power do not exist in isolation and instead can be used in tandem as each activity draws on or strengthens the other dimensions of power (Fuchs 2007). For example, lobbying benefits from the potential threat of relocating investments and jobs (structural power) and self-regulation benefits from businesses’ acquisition of legitimacy as political actors (discursive power) (Fuchs 2007).

Although empirically separate from the three dimensions of business power, regulatory capture (see Chapter 3) can be an outcome of these power dynamics as they often work in concert. In this dissertation, the degree of regulatory capture is treated as the outcome I seek to explain through the data broker industry’s use of the three dimensions of business power. Despite each dimension having a varying degree of success depending on the industry size, regulatory status and use of the three dimensions, differentiating but employing capture theory and the three dimensions of business power in tandem permits an exploration into the ways in which firms create or maintain a regulatory system that benefits their industry.

In addition to shedding light on how key capitalistic actors can influence policymaking, scholars across the literature on the role private actors are paying additional attention to the impact of political salience on business power and policymaking (Massoc 2019). This stream of literature emerged as scholars sought to understand why, in capitalist democracies, powerful business actors sometimes lose (Massoc 2019). They argue that business power varies in function of the political salience, the degree of public attention that one specific issue receives, of the issue at stake (see Bell and Hindmoor 2015; Culpepper 2010; Massoc 2019; Woll 2013). Weapons available to business are dreadfully efficient when they are used away from the public spotlight, however, when public concern rises, firms can no longer count on the deference of politicians as the potential political cost of not listening to them becomes too high (Massoc 2019). Thus, low issue salience and quiet politics generally benefits business interests as the more invested the public is in an issue,

the less organizations can exercise disproportionate influence over the rules governing that issue (Culpepper 2010; Massoc 2019). Put more succinctly, business power decreases as political salience increases (Culpepper 2010). Despite some tools to ensure low salience, firms generally cannot prevent the media or ambitious politicians from exploiting issues to acquire readers or votes (Culpepper 2010). However, for firms that employ highly technical digital processes, one strategy to maintain low political salience is to ensure their business practices are too complex for politicians, journalists and the public to understand. Since this strategy can be especially advantageous for data brokers, this dissertation will be alert to any overtly technical or clandestine data harvesting and monetization techniques.

What differentiates authority from power is the legitimacy of the claims of authority, that is there are both rights claimed by a superior authority and obligations recognized as legitimate by the subordinates or subjects to that authority (Hall and Biersteker 2002). Authority requires a basis of trust rather than a calculation of immediate benefit and, institutionalized cooperation that involves creating shared norms, rules and experiences (Cutler, Haufler, and Porter 1999). In both domestic and international spheres, this authority was previously the prerogative of sovereign states, however, today, the state is no longer the sole or even principal source of authority as private actors are increasingly involved with decision-making (Cutler, Haufler, and Porter 1999; Hall and Biersteker 2002). As states abandon some of the traditional functions that are required for the smooth operation of markets, especially in areas dominated by technology, the private sector can be seen as more capable than governments in designing and maintaining appropriate rules and procedures (Cutler, Haufler, and Porter 1999). Therefore, the frameworks that govern international economic transactions are increasingly created and maintained by the private sector and not by the state or interstate organizations (Cutler, Haufler, and Porter 1999).

Corporations, “singly and jointly, construct a rich variety of institutional arrangements that structure their behaviour. Through these arrangements, they can deploy a form of private authority whose effects are important for understanding not just the behaviour of firms, but also for analyzing the state and its policies” (Cutler, Haufler, and Porter 1999). The concept of private authority is difficult to define, however, a key source of private authority is the process by which interfirm cooperation is routinized and institutionalized over time from the interactions between firms and the interactions between firms and the state (Cutler, Haufler, and Porter 1999). There are six general types of cooperative arrangements (see Table 1) that may be identified as authoritative arrangements in terms of the participants' acceptance of the arrangement as legitimate and their general compliance with their precepts (Cutler 2002). These arrangements include informal industry norms and practices, coordination service firms, production alliances, cartels, business associations and private international regimes. For this dissertation examination of the global data broker industry in Canada, the two most relevant cooperative arrangements are the information industry norms and practices and business associations.

Table 1: Six general types of cooperative arrangements

Cooperative Arrangement	Definition
Informal industry norms and practices	The loosest form of inter-firm cooperation, which often evolves through repeated practices in industries and firms that acquire authority over time.

Coordination service firms	Firms that coordinate the behaviour of other firms, such as stock exchanges, insurance firms and financial clearinghouses.
Production alliances, subcontractor relationships, and complementary activities	Includes strategic partnerships, joint ventures, and networks.
Cartels	Formal and informal arrangements between producers to coordinate their output and prices.
Business associations	Associations can be self-regulatory, developing norms and procedures that bind members or representative, acting on behalf of members for their dealings with governments. They are important for the creation of norms and practices that can evolve into rules of customary international law.
Private international regimes:	An integrated complex of formal and informal institutions that is a source of governance for an economic issue area, such as the WTO.

Contrary to the scholarship on business power and private authority, some scholars postulate that states are still more powerful than firms. These state-centric scholars argue that the idea of a powerless state is a myth as states are still the most important political organizations in the modern world, they are just returning to the heart of economic life in a different way than before the 1980s (Cerny 2010; Weiss 1997, 2018). These authors have attacked the neoliberal thesis that portends the displacement of states as powerful actors in the domestic and international arenas arguing that the greater internationalization of economies has reinforced the role of the state (Bruno 2000). However, non-state actors such as international organizations and enterprises are increasingly acquiring power to the extent that they are legitimated as authoritative (Hall and Biersteker 2002).

Cutler et al propose several explanations, most notably structural power approaches, for the rise of private authority and cooperative arrangements in the international economy. Structural power “confers the power to decide how things will be done, the power to shape frameworks within which states relate to each other, relate to people, or relate to corporate enterprises” (Strange 1988, p. 27). In this approach, social institutions systematically advantage some actors over others as certain actors such as transnational corporations (TNC) become “authoritative as a means to increase their ability to shape and profit from market activity; they are structurally advantaged by the spread of liberal institutions and global capitalism” (Cutler, Haufler, and Porter 1999, p.337). When private sector actors are the major players establishing the rules of the game for a given framework to govern economic transactions, they can be exclusionary and ensure that the rules and market discipline favour or exclude certain participants (Cutler, Haufler, and Porter 1999; Nesvetailova and Palan 2020). Furthermore, these rules can be created by decision makers who are only accountable to an industry, business constituency or the market itself, and not to any citizens or consumers (Cutler, Haufler, and Porter 1999). When state officials concede to the forces of the global market, proclaiming that they have little room to manoeuvre or make independent policy choices, they are participating in the construction of markets as authoritative (Hall and Biersteker 2002).

With the rise of neoliberalism, governance over the last 30 years has primarily been indirect and delivered via various forms of private authority. With technological advances that facilitated the

global exchange of ideas and commercial transactions, new layers of regulation at the national and international levels would emerge, allowing for the creation of co-regulatory constellations between the public and the private (also see Ayres & Braithwaite, 1992). Self-regulation is often a starting point for these constellations as authority is explicitly transferred to private bodies that delineate a sphere of expertise, establish membership conditions, limit competition for non-members and impose rules of conduct (Black 1996; Coglianese and Mendelson 2010).

Beyond self-regulation, intergovernmental organizations such as OECD have been shaping identities, producing knowledge, and controlling the global economy by promoting certain behaviours, norms and ideals that reinforce a particular set of practices that are consistent with its enthusiasm for liberalized markets (Porter and Webb 2008). These OECD practices demonstrates how knowledge is created and the importance of the international flows of knowledge (Porter 1999). When changes in information and financial technologies arise, the basic relationship in any political economy is altered as technological advancements, more than anything else, drives changes in the structures of power (Stopford, Strange, and Henley 1992; Strange 1997). The OECD has been central to the dissemination and widespread implementation of Fair Information Principles and general practices for data protection, both of which shape the structure of information markets and the international economy in general.

This dissertation seeks to identify other forms of private authority that shape the data broker industry in Canada. This will entail determining if there are any norms or discourses promulgated by the data broker industry, identifying any data broker business as well as the examining the role of the WTO and its policies on trading data. With data brokers largely self-regulating, it will be crucial for this dissertation to identify the features of Canada's privacy framework that enable this self-regulation. Using responsive regulation and capture theory, which are discussed in the next chapter, in conjunction with the literature on the role of private actors, this dissertation seeks to investigate the role that data brokerages play in ensuring that their industry remains under-regulated. Central to this investigation will be determining if the lack of regulation is attributed to private actors lobbying the government and capturing regulators or to legislators and regulators who are unaware of data brokers and their business practices or a combination of the two.

With the transborder flows of consumer data and the presence of global data brokerages in Canada, the literature on the role of private actors also permits me to examine the growth and regulation of this industry at the national and international levels. With U.S.-based global data brokerages operating in Canada, it will be imperative for my dissertation to examine how these firms assert their power and influence, capturing regulations to ensure that their interests in buying and selling personal data are continued to be placed above the privacy interest of consumers.

The scholarly works identified and discussed above that comprise the literature on privacy, Big Data and data brokers and business power will be employed throughout the empirical chapters of this dissertation and help guide my examination of the global data broker industry in Canada. Beyond building upon existing knowledge, this dissertation seeks to advances these bodies of literature by identifying and filling gaps. Across the literature on privacy and data brokers there is minimal discussion on whether the business practices of marketing and advertising data brokers violate a specific set of privacy statutes. To fill this gap, this dissertation examines the business practices of data brokers to determine if and how they violate Canada's private sector privacy law.

To do so, this dissertation does not assume that all data brokers violate privacy. Instead, I examine the ways in which data brokers violate and comply with privacy laws and regulations. A second gap this dissertation seeks to fill is the absence of any scholarly literature on the avenues of influence utilized by data brokers to advance their interests. Since data brokers are not consumer facing, are an issue of low political salience and are largely under-regulated, this dissertation identifies the avenues of influence available to data brokers in Canada and examines this industry's uses of the three dimensions of business power.

By examining the global data broker industry in Canada, Canada's privacy regime and the business power data brokers, this dissertation advances and provides a novel contribution to the three bodies of literature discussed in the chapter. With little attention given to Canada, data brokers and data brokers in Canada across these three bodies of literature, this dissertation fills these gaps by calling attention to the business power and practices of an industry that is largely unknown to Canadian policymakers and consumers as well as the laws that enable the growth of the data broker industry.

Chapter 3: Theory and Methods

Introduction

In an era marked by the unprecedented production and accumulation of consumer data facilitated by e-commerce firms, financial institutions, and digital platforms, the discourse surrounding privacy protection and regulatory governance has gained paramount significance. The complex landscape of these issues has been the subject of a growing body of scholarship. However, notably absent from this literature is a comprehensive overview of the data broker industry in Canada and an exploration of the strategies employed by these firms to circumvent or weaken regulations that might otherwise impact their business practices.

To address the research questions presented in Chapter 1 this chapter establishes a unique theoretical framework and methodological approach that when combined, are poised to provide a thorough explanation of the factors that enable and at times encourage the monetization of Canadian consumer data by data brokers. This comprehensive exploration seeks to contribute significantly to the broader discourse on data privacy and regulatory challenges in the Canadian context. In the pursuit of explanations for the inability of privacy legislation and regulations to adequately safeguard personal information in the digital age, novel theoretical and empirical contributions are generated. Therefore, the theoretical framework that guides this dissertation is comprised of three theories that will assist me in developing a comprehensive explanation to address my research questions and support my central argument. Both of which are presented in Chapter 1.

The chapter is organized into two main sections. Section 3.1 presents the unique framework comprised of three complementary theories that guides the empirical investigation undertaken in the preceding chapters. Section 3.2 discusses the methods utilized to collect the data presented in the empirical chapters of this dissertation.

3.1 Theoretical Framework

The lens through which this study examines the interplay of privacy, regulation, and industry dynamics is threefold. Firstly, the economics of privacy provides a framework for examining the implications of privacy practices and trade-offs for firms and consumers participating in information markets. This theory takes consumer behaviour, market forces and the valuation of consumer data into consideration, all of which will be utilized to explain how current data privacy laws favour profits over privacy. Secondly, capture theory offers insights into how regulatory agencies may, over time, become susceptible to industry influence, compromising their ability to act in the public interest. This theory will assist in determining if data brokers have captured regulatory agencies and if this capture has resulted in privacy regulations that put industry interests above the public interest. Lastly, Responsive Regulation offers a theoretical perspective that recognizes the need for regulatory authorities to engage with stakeholders, assess emerging risks, and calibrate their approaches accordingly. This theory will guide the examination of how regulatory bodies can maintain agility and relevance in addressing evolving privacy concerns.

The convergence of these three theoretical perspectives provides a comprehensive lens through which to dissect the intricate relationships between privacy, regulation, and industry

behaviour in the age of big data across four separate yet interrelated levels of analysis (consumer, firm, state and international) that shape the data privacy landscape in Canada.

3.1.1 The Economics of Privacy

The economics of privacy employs economic theories to analyze how individuals, firms and policymakers interact in markets where personal data is exchanged and, the policy implications between individuals' decisions to disclose personal information and firms' strategies to innovate using these data (Cecere et al. 2017). Since the economics of privacy first emerged in the 1970s, the theory has evolved through three waves. The first wave gained traction when laissez-faire scholars from the Chicago school began to view consumer privacy protections and transparency obligations as an "example of perverse government regulation of social and economic life" (Posner 1978). Privacy laws or personal information protections were seen as restrictions on information flows which decreases the quality of information regarding economic agents in the marketplace resulting in an inefficient market, increased costs for firms and a decline in societal and economic welfare (Posner 1978; Stigler 1980). A key finding from this era was that privacy costs and benefits are inextricably related and that privacy is an inefficient and redistributive economic roadblock (Acquisti 2014; Brandimarte and Acquisti 2012).

As the creation of low-cost technologies for data manipulation generated new concerns for personal information processing, a second wave of research in the economics of privacy developed between the 1990s and mid-2000s (Varian 2009). Scholars now focused on the trade-offs for data holders and subjects, the establishment of personal information markets and the economic implications for secondary uses of personal information (Acquisti et al., 2016; Cecere et al. 2017; Varian 2009). The secondary uses data were seen as the primary avenue for which many invasions of privacy occurred, and market failure arose (Laudon 1996). A key similarity between the first two waves is the notion that the mere legal protection of privacy is outdated and a hybrid model that combines markets, technology and regulation is required to satisfy the needs of consumers and firms (K. Laudon 1996; H. R. Varian 2009).

More recently, a third wave has emerged that employs microeconomic modeling to analyze equilibrium in the market for privacy (Brandimarte and Acquisti 2012). The findings suggest that privacy protections (or lack thereof) carry both costs and benefits for data subjects and holders alike, but that when consumers are rational decision-makers, a regulatory regime for privacy protection is not necessary as it is in the firms' best interest to protect consumer data (Acquisti and Varian 2005; Brandimarte and Acquisti 2012; Taylor 2004). The third wave is linked to the economic issues brought forth by the development of various information technologies of the 21st century such as social media and behavioral targeting (Acquisti, Taylor, and Wagman 2016a). With these technological advancements there are multiple dimensions to privacy and economic trade-offs that arise from different angles of the same privacy scenarios (Acquisti, Taylor, and Wagman 2016). With Big Data, it becomes evident that decisions data subjects and holders make about personal information can lower search costs and reduce inefficiencies but also lead to economic inequalities and asymmetries between data holders and subjects (Acquisti 2014).

At its core, this theory is concerned with privacy trade-offs (i.e. disclosing or protecting personal information) for data holders, data subjects and society as a whole (Acquisti, Taylor,

and Wagman 2016). Although disclosing data can carry immediate tangible (receiving a discount) or intangible (“liking” a post) benefits, privacy trade-offs are inherently intertemporal as the cost of sharing data is generally incurred later in time (Acquisti, Taylor, and Wagman 2016). Thus, with these trade-offs both positive and negative externalities arise as sharing or protecting data can either increase or decrease individual and societal welfare (Acquisti, Taylor, and Wagman 2016; Varian 2009). For example, consumers receive personalized services and discounts through loyalty programs by sharing their data with firms. Following these transactions, consumers have little knowledge or control over how their data will be used. Consequently, negative externalities arise when a firm sells or shares its customers’ personal information to a third party who may impose costs, such as spam emails, on the customers (Acquisti, Taylor, and Wagman 2016; Varian 2009).

In addition to evaluating trade-offs, the economics of privacy provides a useful theoretical lens to examine other issues regarding data privacy in the digital age. With the ascent of the Web 2.0 and the growth of data analytics, individuals are no longer simply consumers, but, are instead public producers of highly personal data (Acquisti, Taylor, and Wagman 2016). When examining the collection of individuals’ actions, desires and interests by third parties, often without individuals’ knowledge or explicit consent, through an economics of privacy lens, these attributes are seen to have substantial economic value and are regarded as business assets that can be used to target advertising or be traded with other parties (Acquisti, Taylor, and Wagman 2016; Cecere et al. 2017; Laudon 1996). Buying, selling, trading and exchanging consumer data has resulted in the creation of multiple information markets. These markets “don’t just happen, they arise in a context of social, moral and political understandings” (Laudon 1996). There are information markets where data aggregators trade data with other organizations and markets where consumers exchange personal information for free products and services (Acquisti, Taylor, and Wagman 2016). In the former, consumers are excluded from transactions as they are unable sell or buy back their data and in the latter, consumers implicitly sell their information to access free or personalized services (Acquisti, Taylor, and Wagman 2016).

In these markets, weak consent clauses often fail to give users ongoing control over their data after collection, potentially allowing its use beyond originally stated purposes (Laudon 1996). Consequently, property rights over this information are held by firms and not the individuals themselves. With information markets and large-scale databases, it is cheaper and easier for firms to violate privacy on an unprecedented scale (Laudon 1996; Varian 2009). Thus, the current privacy crisis is not the result of technological progress alone but is derived from market failures that occur when personal information is obtained and used without consent, when individuals are denied property rights over their personal information and when information is inaccurate or misused (Laudon 1996; Stigler 1980).

Similarly to markets, regulations also arise out of certain political, social, and moral contexts. I opine that the failure of existing regulations to protect personal information from data brokers can be attributed to the prioritization of profits over privacy. Therefore, with the economics of privacy, I can investigate and explain how and why trade-offs that attempt to balance profits and privacy prioritize the former while disregarding the latter. This theory will be utilized to identify and examine the dominant economic ideas utilized by both states and firms to create information markets and privacy policies that seek to balance the need for firms to use

data and individuals' desires to protect their data. Additionally, I will use the economics of privacy to examine the ways in which both states and firms justify the collection and monetization of personal information as well as prioritize profits and innovation over privacy.

From Google Maps to Spotify, the exchange of data for services has become a prevalent practice in the digital economy. By agreeing to the terms of service, consumers, willingly or not, become participants in various information markets. The act of exchanging data for personalized services is not inherently problematic; in fact, it can be beneficial as not paying for multiple monthly subscriptions can yield numerous financial, social, and psychological advantages for consumers. However, concerns emerge when consumers exchange their data for services based on weak notice and consent terms filled with technical jargon and legalese that fail to stipulate how their data will be used and by whom. As data collection becomes more invasive and ubiquitous with the growth of the data driven economy it is imperative to determine how these enduring economic perspectives are shaping privacy statutes and regulations in Canada in ways that encourage the collection and monetization of personal information.

When personal information is sold or exchanged among third parties, such as data brokers, individuals lose control over their data and are unable to provide consent for the secondary use of their personal information. Although the use of personal information without consent predates the digital age, technological advancements of the digital age such as big data, machine learning and AI have exacerbated individual's loss of control over their personal information.

Recognizing the value consumers find in exchanging their data for services, I will employ the economics of privacy to elucidate how privacy and information markets function in practice. This framework, coupled with responsive regulation and capture theory, will aid in illustrating how current regulatory models and privacy statutes have overstated consumers' abilities to assess privacy trade-offs, particularly in the realm of Big Data and AI, and have become overly reliant on self-regulation. Additionally, I aim to problematize the economics of privacy and more specifically, economic assumptions of privacy, as a contributing factor for the under-regulated data broker industry in Canada. With this distinctive theoretical framework, I aim to provide an unparalleled analysis of the business practices of data brokers and their role in the breakdown of information markets.

3.1.2 Capture Theory

From the impact of banking regulations on income inequality (Manish and O'Reilly 2019) to the assignation of penalties in National Hockey League (NHL) games (DeAngelo et al., 2018), capture theory is a useful tool to examine how special interest influence can shape policies, regulations, and/or rules across various industries and issue areas. Capture theory garnered significant attention following George Stigler's (1971, p. 3) observation that "as a rule, regulation is acquired by the industry and is designed and operated primarily for its benefit". Stigler challenged the public interest perspective that government intervention arises from well-meaning politicians and regulators seeking to protect consumers from monopolistic abuse by asserting that even when a regulatory agency is established to avert abuse, regulation can be 'captured' by regulated entity (Dal Bó 2006; Manish and O'Reilly 2019). Applying the principles of supply and demand to regulation, Stigler viewed the legislature or regulatory agency as the supplier and a group (normally businesses) that anticipates benefits from the regulatory program as the demander (Posner 2013). Stigler

emphasized that regulation was supplied in response to the demands of interest groups struggling among themselves to maximize the incomes of their members (Posner 1974). The Stiglerian account of capture focuses on entry-barrier capture, with regulators intervening in markets to privilege one set of producers over another, whereas today, capture is better associated with deregulation or weakened regulation (Carpenter 2013a).

Since 1971, many scholars in political science and economics have contributed to the literature on capture theory by providing definitions of capture. For Richard Posner (2013, p. 49) capture “refers to the subversion of regulatory agencies by the firms they regulate” where the regulated firms have waged and won the war against the regulatory agency, turning the agency into their vassal. David Engstrom (2013, p.31) defines capture as “the process by which policy is directed away from the public interest and toward the interest of a regulated industry.” Lastly, for Ernesto Dal Bó (2006, p. 203), capture is “the process through which special interests affect state intervention in any of its forms, which can include areas as diverse as the setting of taxes, the choice of foreign or monetary policy, or the legislation affecting research and development.” Despite these noteworthy conceptual contributions, a universally accepted definition of capture remains elusive.

In the pursuit of a comprehensive framework for assessing regulatory dynamics, it is imperative to adopt a precise definition of capture. For this dissertation, I will be employing the following definition articulated by Carpenter and Moss (2013, p. 13) whereby regulatory capture “is the result or process by which regulation, in law or application, is consistently or repeatedly directed away from the public interest and toward the interests of the regulated industry by the intent and action of the industry itself.” I opted for this definition of capture due to Carpenter and Moss’s incorporation of “repeatedly directed away from the public interest”.³

Capture theory provides several key mechanisms to examine the intricate dynamics at play within a regulatory landscape and explain why capture occurs. First, information asymmetries can lead to regulatory capture, as regulators require access to industry-specific information to carry out their duties yet much of this information is possessed by the regulated firms (Zingales 2013). The absence of explicit disclosure requirements opens avenues for implicit reciprocity arrangements, where regulators make certain concessions to firms in exchange for the information they require (Zingales 2013). The discretion exercised by regulators is dangerous as the firm may tempt the regulator not to disclose information to their regulatory agency that would be harmful to their business practices (Dal Bó 2006). Ultimately, the extent of capture of the regulator by the firm is contingent upon the amount of information the regulator may obtain and the extent to which the regulatory environment permits bribes (Dal Bó 2006).

Incentives constitute a secondary dimension of regulatory capture, as firms offer both positive and negative incentives to regulators. Positive incentives may include bribes, campaign contributions, or promises of future employment within the industry, enticing regulators to align with industry interests (Dal Bó 2006). Conversely, negative incentives could involve threats (tacit or explicit), rumours to tarnish a regulator's career, or open confrontation to raise the political costs of a government supporting the regulator (Dal Bó 2006). Regulatory capture is widespread primarily because standard economic incentives are deeply embedded in regulatory roles, and many coveted

³ It is imperative to acknowledge the invaluable contributions of numerous scholars who have previously delved into the multifaceted aspects of capture, and their insights continue to inform the discourse on this subject.

positions for regulators are found within the very industries they oversee, compelling even the most well-intentioned regulators to cater to the regulated (Zingales 2013).

Identifying the mechanisms and features of the regulatory landscape that can lead to capture is necessary but not sufficient for determining if a regulatory agency has been captured. To diagnose capture, one must posit a defensible model of public interest, identify a policy shift away from the public interest toward industry interest and show both action and intent by the regulated industry (Carpenter 2013b). If this systematic process determines that a regulatory agency has been captured, the diagnosis is not yet complete as capture is not “all or nothing”. Instead, capture theory acknowledges that there are varying degrees of capture ranging from strong to weak. Strong capture “violates the public interest to such an extent that the public would be better served by either (a) no regulation of the activity in question – because the benefits of regulation are outweighed by the costs of capture, or (b) comprehensive replacement of the policy and agency in question” (Carpenter and Moss 2013, p. 11). By contrast, weak capture “occurs when special interest influence compromises the capacity of regulation to enhance the public interest, but the public is still being served by regulation, relative to the baseline of no regulation” (Carpenter and Moss 2013, p. 12).

Understanding the degrees of capture is essential for both policymakers and scholars, as it allows for a more comprehensive analysis of regulatory dynamics within specific industries and agencies. To diagnose regulatory capture and identify the avenues through which data brokers can advance their industry interests, Doris Fuch’s three dimensions of business power (see Chapter 2) can be employed. Although this conception of business power is empirically distinct from regulatory capture, firms and industries can utilize instrumental, structural and discursive forms of power to consistently and repeatedly redirect laws, policies and regulation away from the public interest and toward industry interest. In other instances, there is an alignment of commercial and business interests (structural power) that significantly reduces the need for firms and/or industries to capture both legislators and regulators as the promotion of self-regulation and profit making are entrenched features of the capitalist economic system. Thus, in this dissertation, regulatory capture is treated as an outcome of firms and/or industries employing their three dimensions of business power to create or maintain a favourable regulatory environment.

One challenge with the capture scholarship is the lack of nuance in describing how and to what degree capture works in particular settings (Carpenter and Moss 2013). When capture is spoken about in the regulatory context it is assumed that is unidimensional - either you are captured, or you are not (Makkai and Braithwaite 1992). The regulatory world is one of shades of grey. Yet capture scholarship does not typically differentiate between these shades in ways that enable informed advice on the marginal value of regulatory (or deregulatory) policy options (Carpenter and Moss 2013). Therefore, I will leverage the understanding of the degrees of capture to conduct a comprehensive analysis of the intricate landscape of the data broker industry to first determine if there is evidence of capture, and if there is, whether the capture is strong or weak.

Since Canada’s privacy regime consist of national and sub-national statues and regulations, there are multiple privacy regulations that can be directed away from public interest and toward private interests. If I can demonstrate that privacy regulations have repeatedly been redirected by data broker lobbying to serve and promote their interests, I can then conclude that there is a strong, degree of capture. Additionally, my claim of a strong degree of capture could be further substantiated

if I am able to determine the action and intent of the data broker industry in redirecting regulations. Conversely, if there is limited evidence of regulations being redirected or weakened, then I conclude that there is a weak degree of regulatory capture. However this does not necessarily mean that the industry is well-regulated since other features of business power than regulatory capture may contribute to an absence of regulation.

Following a diagnosis of the presence or absence of capture, I can then examine the mechanism through which regulatory capture or its absence unfolds and contributes to the strong or weak degree to determine the impact that information asymmetries, incentives and the revolving door, or a combination of the three, can have on regulatory outcomes. This examination will simultaneously expand the use capture theory to an industry where it has yet to be employed and contribute valuable insights into a growing industry that has been largely excluded from the literature on private interest influence and regulation. In areas such as data privacy and consumer protection, even the weakest form of capture can produce regulatory outcomes that favour the interests of data brokers at the expense of consumers, and other forms of business power may be sufficient to achieve the industry's goals without having to engage in regulatory capture.

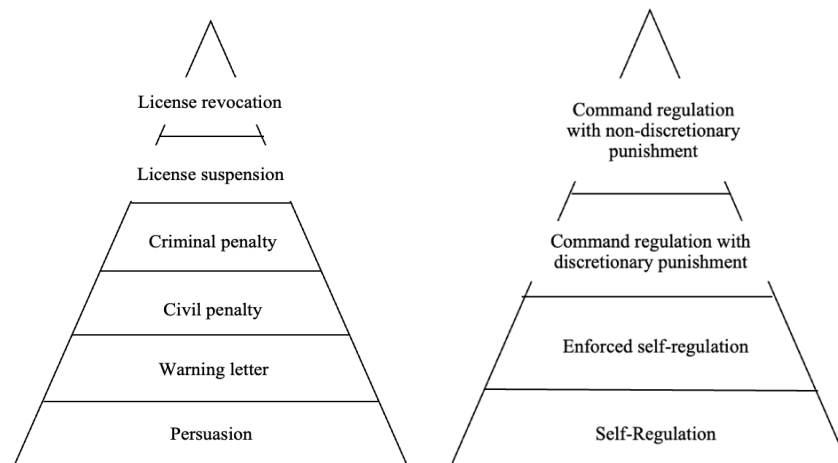
3.1.3 Responsive Regulation

Responsive regulatory theory was developed by John Braithwaite as a theory of business regulation. Since then, this theory has been applied to a wide range of private and public governance applications (Braithwaite 2012). As a product of the early 1990s, responsive regulation reconciled economic theories of regulation, such as rational choice and incorporated major insights into game theory (Braithwaite 2012). In *Responsive Regulation: Transcending the Deregulating Debate* John Braithwaite and Ian Ayres break the contest between stronger regulation of business and deregulation and move the regulatory enforcement debate beyond the dichotomy of either deterrence or compliance. In doing so Ayres and Braithwaite (1992, p. 3, 25) state that “Good policy analysis is not about choosing between the free market and government regulation” as “the trick of successful regulation is to establish a synergy between punishment and persuasion.” Thus, the basic idea of responsive regulation is that governments should be responsive to the conduct of those they wish to regulate and before escalating interventions, regulators should first be responsive to how effectively an entity (i.e. citizens or corporations) are regulating themselves (Braithwaite 2002).

The most distinctive aspect of responsive regulation is the regulatory pyramid (Braithwaite 2002). The pyramid is a range of enforcement sanctions from persuasion and civil penalties to criminal penalties and license suspensions (Ayres and Braithwaite 1992). A core feature of pyramid is that compliance is more likely when a regulatory agency operates an explicit regulatory pyramid. For firms, Ayres and Braithwaite present the enforcement pyramid and for industries, they advance the enforcement strategies pyramid (see Figure 1). For Ayres and Braithwaite (1992, p. 103), self-regulation “is an attractive alternative to direct government regulation since the state cannot afford to do an adequate job on its own”. If the free market and self-regulation fails to protect consumers, regulators can escalate to enforced self-regulation which involves negotiations between the state and firms that result in flexible, particularistic standards and enforcements (Ayres and Braithwaite 1992). More specifically, enforced self-regulation is a “form of subcontracting regulatory functions to private actors” where regulated firms take on some or all of the legislative, executive and judicial regulatory functions, devising their own regulatory rules,

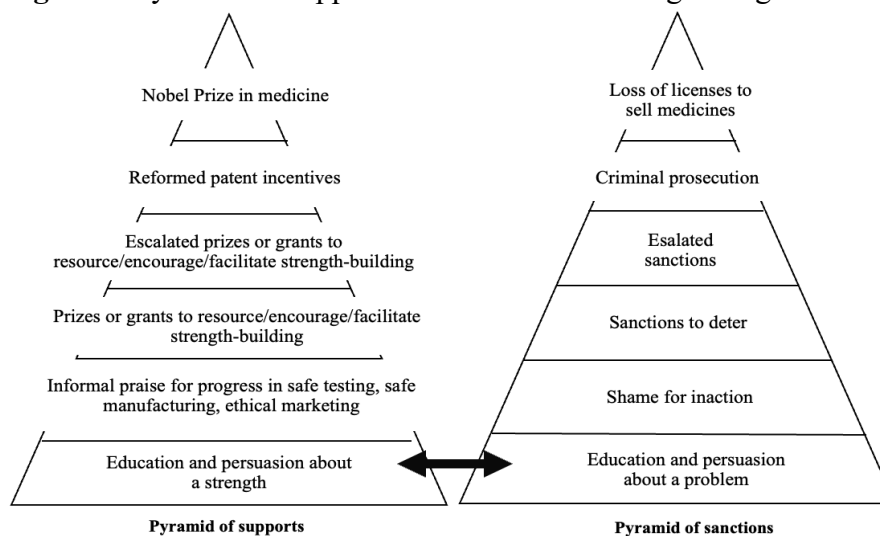
monitoring themselves for noncompliance and correcting noncompliance (Ayres and Braithwaite 1992, p. 103). However, to make self-regulation effective it must be embedded in schemes of escalating measures (Ayres and Braithwaite 1992).

Figure 1: The Enforcement Pyramid and The Enforcement Strategies Pyramid



In addition to the enforcement pyramids, regulators can move up and down pyramids of supports and sanctions to encourage positive behaviour and can escalate to more punitive measures in the event of non-compliance (Braithwaite 2012). Figure 2 is an example of a pyramid of supports and sanctions for the regulation of medications in

Figure 2: Pyramid of Supports and Sanctions for Regulating Medicines



Braithwaite, John. (2011). "The Essence of Responsive Regulation." Pg 482

Australia. Since persuasion does fail, escalation up the pyramid through progressively more severe penalties will take the rational calculator to a point where it becomes rational to comply because the gains from breaking the law no longer outweigh the costs of following the law (Braithwaite 2002, 2012). However, it is also important to note that the successive failure of deterrence measures in business regulation can be attributed to management not possessing the necessary competencies to comply (Braithwaite 2002). To address the failures of persuasion and deterrence measures, responsive regulation expects, encourages and at times requires continuous improvement in discovering lower-cost ways to achieve regulatory goals and better outcomes (Braithwaite 2012). By establishing a synergy between punishment and persuasion where sanctions are kept in the background and regulations are transacted through moral suasion, the

more effective the regulations will be (Ayres and Braithwaite 1992). Being responsive allows regulators to tailor, and amend the pyramids presented below to implement regulations that specifically target the actions of firms and industry-wide behaviours that they seek to curb collaboratively without immediately resorting to punitive measures.

By asserting a willingness to impose more intrusive regulations, responsive regulation can channel marketplace transactions to less intrusive and less centralized forms of government intervention while escalating forms of responsive regulation can retain the benefits of laissez-faire governance without abdicating the government's responsibility to correct market failure (Ayres and Braithwaite 1992). To counterbalance the potential threat of regulatory capture and corruption at the hands of corporate lobbying, Ayres and Braithwaite advocate for a system of tripartism where Public Interest Groups (PIGs) and citizens associations are legally empowered parties within the regulatory process that can act as informed representatives of regulatory beneficiaries (Ayres and Braithwaite 1992; Baldwin, Cave, and Lodge 2011).

The incorporation of multiple stakeholders in responsive regulation leads to a networked escalation pyramid whereby a wider range of partners are included as regulators move up the pyramid, demonstrating the regulators do not stand alone in their concerns for consumer protection (Braithwaite 2012). Engaging a wider network of partners places additional pressure on the regulated firm or industry, further increasing the chances of compliance (Braithwaite 2012). Responsive regulation has been and continues to be an influential policy idea because it formulated a way of reconciling the empirical evidence that "sometimes punishment works and sometimes it backfires-and likewise with persuasion" (Braithwaite 2012, p. 48). Placing heavy reliance on persuasion measures and self-regulation first as opposed to punishment is important for industries where technological and environmental realities change so rapidly that detailed, hard law-orientated regulations cannot keep up to date (Ayres and Braithwaite 1992).

In this dissertation, I aim to apply responsive regulation theory in three distinct ways. Firstly, the theory will be employed to examine and explain the limitations of existing national privacy statutes in safeguarding consumers, as well as the absence of regulation governing the business practices of data brokers in Canada. A contributing factor to this issue lies in the prevalent reliance on self-regulation across the tech sector to foster innovation and prevent regulations from becoming obsolete with technological advancements. Through responsive regulation, it becomes apparent that firms are exploiting self-regulation, necessitating an escalation an up the enforcement strategies pyramid. However, increased state intervention in the business practices of data brokers has not manifested in the form of support or sanctions.

Second, I will employ responsive regulation alongside capture theory and the economics of privacy to assess whether and to what extent data brokers have influenced the regulation of their industry to maintain the status quo of self-regulation. Given that data brokers handling the data of Canadian citizens may not necessarily be incorporated or located in Canada, it is imperative for this project to evaluate how these firms navigate Canadian privacy laws and whether they impact privacy regulations in Canada. Additionally, I will investigate the existence of cooperative arrangements such as industry associations within the data broker industry that may assist these firms in influencing regulation, as well as any public interest groups seeking to counter this influence and hold these firms accountable.

Lastly, I will present responsive regulation as a useful approach for addressing the under-regulated global data broker industry in Canada. After examining the gaps in Canada's privacy regime that enable the data broker industry (Chapter 5) and the formal lobbying activities of data brokers (Chapter 6) I will discuss how a responsive regulatory approach can address these gaps and any regulatory capture. This discussion will be centered around applying responsive regulation to Canada's existing privacy regime and enforcement model as this dissertation aims to provide an enduring contribution to the literature.

3.1.4 Theoretical Approach

The synthesis of the economics of privacy, capture theory, and responsive regulation forms a distinctive and comprehensive theoretical framework that will be used to examine Canada's privacy regime and under-regulated data broker industry. To do so, this theoretical framework presented in this chapter makes several original and important contributions to the application and understanding of these theories as well as to the growing body of scholarship on data-driven economies. An initial distinctive contribution of this framework lies in the amalgamation of these three theories to investigate an industry, with a secondary contribution arising from the use these of theories to examine the operations of the data broker industry. A tertiary contribution of this framework and dissertation will be employing the economics of privacy to the data broker industry and to this industry in the Canadian context.

Through the combination of the three theories outlined above, I aim to diagnose a problem (economics of privacy), identify the consequences of this problem (capture theory), and then present a solution to this problem (responsive regulation). In this dissertation, I will employ the economics of privacy to explain why existing data privacy statutes and regulations inadequately protect the personal information of consumers from data brokers. When examining the current privacy landscape in Canada using this theory it becomes evident that consumers are perceived as capable of making informed decisions about their privacy preferences; self-regulation is deemed paramount, and market failures arising from privacy violations should not be met with stronger laws or new regulations (Cecere et al. 2017; Laudon 1996). Thus, using the economics of privacy to study the costs and benefits associated with the disclosure and protection of personal information for data subjects, data holders, and society as a whole (Acquisti, Taylor, and Wagman 2016), it becomes apparent that privacy statutes and laws in Canada prioritize profits over privacy.

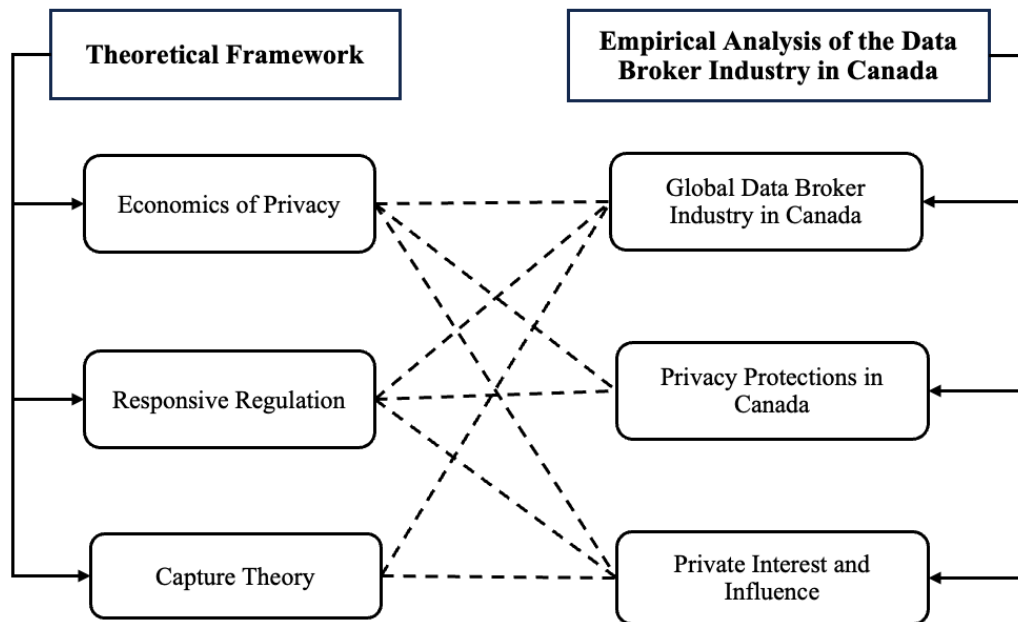
With Canada's federal privacy statute relying on quasi-self-regulation and non-prescriptive principles, many firms, such as data brokers, have been left to collect and monetize personal information with minimal government oversight or intervention. By not being responsive to the data monetization practices of firms in the digital age, federal privacy regulators are failing to safeguard personal information, encourage compliance and escalate to sanctions for noncompliance. To maintain this status quo and/or prevent the enactment of new privacy statutes firms can exercise their business power to influence and shape the policymaking process. If these laws and regulations are repeatedly weakened or redirected away from the public interest, such as the desire to be let alone, a diagnosis of strong regulatory capture can be given.

Using the literature on private interest influence and business power I will identify and examine any avenues through which data brokers exercise their power to determine if regulatory

capture is present and if so, to what degree. In the absence of a strong diagnosis, this dissertation highlights how firms and/or an industry can not only survive, but thrive, without capture. Given the alignment of commercial and government interests, self-regulation and the maximization of profits, firms need not act intentionally to advance their interests as their power is in part produced by these features of a capitalist economic system (i.e. structural power).

To illustrate the bridge between theory and empirics, Figure 3, outlines the primary and secondary connections between the three theories presented in this framework and the four empirical chapters of my dissertation.⁴ In the diagram, the three central tenets of each theory have been outlined to depict how the distinct components of the theories will be employed across the empirical chapters. This delineation highlights the use of each theory in every empirical chapter, showcasing the efficacy of this distinctive framework for investigating my research question, interpreting findings, substantiating my central argument, and providing a significant advancement to the scholarship on these theories. Moreover, this unique framework presents a novel contribution to the limited yet expanding body of research on data brokers.

Figure 3: Connections between Theoretical Framework and Empirical Chapters



3.2: Methodological Approach

To address the three research questions presented in Chapter 1 a mixed-methods approach was utilized. The qualitative component involved desk research and conducting semi-structured elite interviews. A descriptive quantitative analysis was then undertaken to examine the formal lobbying activities of data brokers in both the U.S. and Canada. A detailed account of these

⁴ The diagram presented in Figure 3 was derived from a similar diagram presented in Acquisti et al. 2016. “The Economics of Privacy.” *Journal of economic literature* 54(2): 442–92 that sought to illustrate the connections between the economics of privacy theory and their empirical analysis of privacy.

methods is presented below. Each stage of the research process that guided this dissertation, from participant selection to data analysis, is outlined in this section.

This research commenced with comprehensive desk research through which I collected and examined various primary and secondary sources regarding data, privacy and data brokers from both Canada and abroad. The primary sources I collected and analyzed primarily pertained to the collection, use, and protection of personal information. Specifically, I examined the privacy policies of various B2C firms and data brokers, guidelines promulgated by organizations such as the OECD, national and sub-national privacy statutes, regional and bilateral trade agreement provisions on digital trade, and transcripts from House of Commons Standing Committee meetings. In addition to these primary sources, I also analyzed various secondary sources including academic books and journal articles, online print media articles (from both newspapers and magazines), and grey literature (from think tank and government reports).

To complement this desk research and to gain in-depth knowledge of the uses and regulation of personal information by firms, I conducted 14 semi-structured elite interviews. More specifically, I interviewed academics, marketing executives and directors, privacy professionals, small business owners, and lobbyists. Elite interviews were utilized to incorporate the attitudes, values, beliefs, and first-hand knowledge of experts in my dissertation (Goldstein 2002). Through these interviews I obtained a better understanding of industry trends, the value of consumer data and the realities of lobbying. Since the data accumulated from elite interviews can rarely be considered in isolation, this method contributes to the research goal of triangulation as it allows researchers to compensate for the lack or limit of previously collected evidence and corroborate previously established knowledge (Tansey 2007). With the small yet growing body of literature on the data broker industry, especially in Canada, the data collected from these elite interviews provided invaluable insights that were utilized thorough the three empirical chapters.

In addition to these 14 elite interviews, I spoke with sales representatives and account managers from 4 data brokerages. To complete this doctoral project, it was imperative that I incorporate the first-hand knowledge and experience of individuals employed by various data brokers. After contacting numerous data brokerages requesting interviews and receiving no responses, I developed and employed a novel methodological approach. When looking on the websites of data brokers, many offer a free sample of their data, a ‘30-day trial’ to test and access their products or to view their products and/or services. To access these offerings, a first and last name, email address, and most times, company information must be provided. Shortly after commencing a free trial or accessing a data sample, an account manager or sales representative from that company reaches out via email to “set up a call to discuss your options” or “to find a time to chat about our products”. Following this initial interaction, I spoke with the sales representatives and account managers over the phone and via email. In these conversations I exclusively inquired about their firm’s data products and services, the cost to license or partner with the firm, where the data is sourced from, and if the data was collected in a manner compliant with Canadian privacy laws. At no time during these conversations were the personal opinions, perspectives or positions of the sales representatives and account managers discussed.⁵

⁵ Additional MREB approval was obtained to utilize this method of data collection.

To compile the Data Brokers in Canada List, discussed in Chapter 4 (presented in Appendix A), and identify firms to contact for interviews I employed three approaches. First, in the U.S., several states, such as California and Texas, maintain a data broker registry.⁶ I commenced by determining which firms on the registry operate in Canada. To do so, I examined the firms' products, services and offerings to identify any mention of Canadian consumer data. I also searched for any Canadian offices, branches or locations. From there, I cross-referenced the firms on California's registry with the membership lists of various Canadian advertising industry associations. Since there are data brokers that exclusively operate in Canada, these membership lists were also used to identify these firms. Second, using data marketplaces such as Datarade and Snowflake, where data brokers, retailers, and other B2C firms can list their data products, I searched for firms selling or licensing Canadian consumer, behaviour and location data. Lastly, I searched for and identified Canadian based data brokers, loyalty programs and AdTech firms that profit on the collection and sale of consumer data. With these methods, I have identified over 150 data brokers operating in Canada. Using this list I also made several attempts to determine what data brokers are in possession of my personal information and the types of information they have gathered. An example of this experiment is presented in Chapter 5.

To examine the formal lobbying activities of data brokers, I utilized the federal lobbying data published by OpenSecrets (U.S.) and the Office of the Lobbying Commissioner of Canada to search for the data brokers identified on the Data Brokers in Canada List and California's registry. In the absence of any provincial registries in Canada and federal registries in either Canada or the U.S., a multi-level analysis of data broker lobbying was conducted. To evaluate the formal lobbying of data brokers in the U.S., I searched OpenSecrets for the lobbying activities of the over 500 data brokers on California's registry. I selected to use California's registry to represent the American data broker industry because it is the most populous U.S. state and the home to Silicon Valley, which is where many digital age data brokers (a typology presented in Chapter 4) are headquartered. To examine data broker lobbying in Canada, I searched the Office of the Lobbying Commissioner of Canada's lobbying registration and monthly communication reports data sets for the firms identified on the Data Brokers in Canada list. While not exhaustive of every data broker operating in either Canada or the U.S., these compiled lists nonetheless a useful and valuable dataset for examining the formal lobbying activities of data brokers.

To complete this analysis, I first identified which firms on each list lobbied the Canadian and American federal governments. From there, I focused on formal lobbying related to privacy, consumer protection and digital trade. I then identified the number of lobbying registrations; the money spent on lobbying (U.S. only) and the government officials that were lobbied (Canada only). The purpose of this analysis was to determine if the data broker industry in Canada is under-regulated due to formal lobbying and a strong degree of regulatory capture or the government's limited knowledge on this industry and its operations. The individual country comparative analyses of formal data broker lobbying are presented in Chapter 6.

⁶ The California Data Broker Registry can be found here: <https://oag.ca.gov/data-brokers>

Chapter 4: Monetizing Consumer Data: The Firms and Business Practices of the Data Broker Industry

Introduction

British mathematician Clive Humby said “Data is the new oil. Like oil, data is valuable, but if unrefined it cannot really be used” (Humby 2021)⁷. Similar to oil, data is also a commodity that is traded on global markets and used across various industries. Developing alongside but in the shadows of Big Tech, the Internet, and the digital economy is the data broker industry, which is comprised of firms that collect and monetize consumer data. Once refined, consumer data can be used to derive insights that drive customer retention, new revenue models, and targeted advertising, ultimately leading to increased profits (Talagala 2022). The data broker industry not only survives but thrives because firms are willing to spend money to track, target, and learn their customers’ behaviours and preferences in hopes of increasing their profits. As one marketing executive stated in an interview, “If a third party has good data, we could use to improve response rates by 10 per cent, that is worth it. There is an ROI (return on investment) on everything, that is why the data is so valuable.”⁸

As firms increasingly rely on consumer data to drive insights and profits, free trade agreements have begun to play a pivotal role in shaping the landscape of cross-border data flows. These agreements often include chapters on digital trade or e-commerce with provisions that aim to reduce trade barriers, facilitate the free flow of information and promote consumer trust in firms. The intersection of digital trade, data flows, and consumer privacy presents a wicked policy problem, both internationally and domestically. For states and firms, the ubiquitous collection and monetization of consumer data can lead to increased profits and economic growth. Comparatively, this new logic of accumulation known as surveillance capitalism raises privacy and autonomy concerns for consumers whose personal information, preferences and behaviours are used to create prediction products (Zuboff 2015). These prediction products, which anticipate consumers’ future and current choices are then traded on behavioral futures markets by surveillance capitalists who sell certainty to their clients (Zuboff 2020).

Going beyond firms or surveillance capitalists who sell certainty, this dissertation focuses more broadly on data brokers that monetize personal information for a variety of purposes. This can include providing personalized services, developing new products or identifying new customers. Moreover, since selling a product or service is not the only way for firms generate profits, this dissertation examines the other business models and revenue streams employed by data brokers. For example, beyond the one-time sale of a product, data brokers can lease, license, trade or offer a pay-as-you-go models for their products and services. With these varying business practices and revenue streams, it is becoming increasingly difficult for regulators to safeguard personal information and for consumers to understand how their data is collected, used and disclosed.

In support of this dissertation’s central argument, which states that data brokers in Canada are under-regulated due to Canada’s privacy regime that prioritizes profits over privacy coupled with

⁷ This quote highlights the commodification of data and the importance of data processing. However, what Humby fails to acknowledge is that unlike oil, data is a reusable and renewable resource.

⁸ Interview a marketing executive conducted on May 6th, 2024.

the Government of Canada's limited knowledge on the industry, this chapter provides a comprehensive overview of the global data broker industry and its operation in Canada by identifying firms that comprise this industry, the types of data they collect and their data collection methods. To provide further insights on the data broker industry and its operation in Canada, this chapter presents a unique six-category typology of firms that monetize personal information beyond solely buying and selling and a novel list of the data brokers operating in Canada. Alongside this overview, Chapter 4 examines the ways in which the data broker industry's complexity, clandestine operations and relationship to digital trade create significant challenges for effective national regulation, resulting in the reliance on self-regulation and limited oversight by Canadian regulators and legislators.

The chapter is organized as follows. Section 4.1 discusses the business practices of traditional data brokers, i.e., firms that buy and sell consumer data. Section 4.2 presents the digital age data broker typology and expands on the business practices and firms that fall under each of the six categories. Section 4.3 presents the Data Brokers in Canada List which identified over 150 firms, both domestic and global, that monetize Canadian consumer data. This section also highlights the challenges in regulating a truly global industry and protecting privacy in an era dominated by eliminating barriers to digital trade.

4.1: Data Brokers and the Data They Sell

Data brokers are not all the same. Depending on the information they monetize, data brokers can fall into one of two categories. First, there are data brokers that create and monetize profiles of corporate contacts to assist firms in generating leads. B2B data brokers such as Lusha, sell lists that contain the first name, last name, job title, seniority, emails and phone numbers of 45 million businesspeople in North America (Lusha 2024). Second, there are data brokers that collect, buy and sell consumer data. Given this dissertation's examination of privacy and consumer data I will primarily focus on the consumer-oriented data brokers. With various types of personal information, data brokers can be further divided into four categories.

One, financial information, risk mitigation or fraud prevention data brokers trade personal financial information such as credit scores and financial riskiness (Latto 2020). Appriss Retail, for example, combines point of sale transactions and criminal background information to assist retail managers in evaluating the risk of an employee committing fraud (Kak and Meyers-West 2023). Firms specializing in financial risk analysis including credit bureaus, such as Transunion and Equifax, insurance companies and identity verification services, are some of the biggest players in the data broker industry (CIPPIC 2018a). Two, personal health information brokers, such as IQVIA, compile and build profiles of perceived health issues using online symptom searches and pharmacy purchases (Latto 2020). Pharmaceutical companies are the main clients for health information brokers as they use the data for market research, drug development, marketing, and monitoring drug adherence (Spithoff et al. 2022b). Three, people search data brokers, such as Spokeo and PeekYou, charge a fee to search an individual by name and receive their address, phone number, email address, and date of birth. Four, marketing and advertising data brokers collect and examine information regarding the wants, needs, desires and interests of consumers, and exchange that information to companies looking to sell specific products and services to consumers (CIPPIC 2006). The biggest global names in this category include Acxiom, CoreLogic and Epsilon. Given the focus and scope of this dissertation, I will concentrate primarily on the marketing and advertising data brokers.

As data monetization has become a lucrative business practice in the digital age, data brokers are working to acquire data through any possible means. Despite having a diverse range of sources, methods and partners, as a group data brokers operate at the heart of the expanding industry of commercial surveillance (Crain 2018). Prior to the IoT, cashless economy and social media, data brokers obtained information from newspaper and magazine publishers, book, music, and movie clubs, mail order retailers, service providers, surveys and contests, travel agencies, product manufacturers (via registration/warranty cards), payment processing companies, seminars and conferences, websites, and non-profit and charitable organizations (CIPPIC 2006). Today, data brokers collect information from both off and online sources. Offline, data brokers collect publicly available information such as marriage licenses, arrest records, property sales, and obituaries while online, they scrape publicly available information, track shopping habits, trace IP addresses or cellphones and collect personal information exchanged to use free services such as search engines and social networks (Latto 2020; McClelland 2021). Data brokers can also employ various web-based tools such as cookies or web beacons to track and aggregate consumers' activity across the Internet.⁹ However, with the rise of cookie banners and the denouement of third-party cookies, data brokers, advertisers and B2C firms need to leverage data from more direct sources.

Sources of data can be categorized into one of four parties based on the relationship between a firm, a customer and their data. The definitions of zero, first, second and, third party data presented below were taken from some of the largest data brokers in North America. Zero-party data is the data a customer proactively or voluntarily shares with a brand through social media, interactive quizzes, messages with chatbots, contests or surveys (LiveRamp 2022; Tinuiti 2021). First-party data is collected directly from customers through purchase history, contact information (phone, email or address), subscription information or placing a pixel on a website, app or social media channel (Eplison Marketing 2023). This data is cost-effective, highly accurate and easy to manage (Eplison Marketing 2023). Second-party data is first-party data of another firm. Specifically, it is the data that two or more parties decide to share privately for mutual benefit (Acxiom 2024). Second-party data allows firms to “build a layered and more complete view of individual customers that drives far more relevant, meaningful and personalized marketing that can improve engagement and marketing ROI (Acxiom 2024). Lastly, third-party data is data that is collected or purchased from various platforms and websites where it was originally generated and is purchased from third-parties such as data brokers, (Lotame 2019). To effectively utilize these sources of data, it must be further refined based on the type of information it provides.

To target a specific demographic or provide personalized services, Oracle Digital Experience Agency (2022) has identified seven consumer attributes to categorize personal information. The seven customer attributes are as: demographic, firmographic, technographic, geographic, psychographic, behavioural and social influence (see Table 2). With data brokers, many focus on a select few attributes. For example, Redmob, a Singapore-based location and demographic data broker collects data from more than 50 sources for 1.5 billion devices covering 123 countries to provide clients with real-time insights on consumers' country, city, latitude and

⁹ Web beacons, also referred to as GIFs, pixel tags, or tracking pixels, are small images not visible to the human eye that are embedded in web pages or emails to monitor a user's activity, track their behaviour and follow their online journey. Web beacons work similarly to cookies by tracking Internet browsing. However, unlike cookies web beacons cannot be declined and users are not notified of their use (Croft and McNally 2023).

longitude, location accuracy in meters, IP address, browser language, gender, year of birth and MAID (Mobile Advertising ID) (Datarade and Redmob 2024). Redmob generates 5,580,909,119 pings per month from devices in Canada. From these pings, Redmob has captured 5,411,826,014 events with IP-derived location data and 169,083,105 events with GPS-derived location data.¹⁰ Given Canada’s population of 41 million inhabitants as of March 2024 and the monthly pings recorded by Redmob, it can be inferred that Canadian devices are pinged on average 136 times per month or 4.5 times per day. For firms seeking to connect with their ideal users in Canada through audience analytics, behavioural targeting and real-time bidding, the IP (internet protocol) and GPS (global positioning system) location data, along with the consumer attributes listed above can be licensed annually from Redmob for \$50,000 (USD) (Datarade and Redmob 2024).

Table 2: Seven Types of Consumer Attributes

Attribute	Description	Types of Data
Demographic	Information about who the customer is, and the people associated with the customer	Name, education level, age, credit score and marital status of customer. Names, ages, and birthdays of family members, pets and co-workers
Firmographic	The organization the customer works for	Organization’s name, locations, revenue and scale of operation
Technographic	The technology owned or used by the customer	Browser type and email inbox apps
Geographic	Where the customer or prospect is located	Location of primary home, office, vacation home, and proximity to various points of interest
Psychographic	Why the customer does things	Activities, interests, attitudes, values, lifestyle, and social status.
Behavioural	What the customer or prospect has done	Purchase history, subscriptions, and brand satisfaction
Social Influence	Customers’ reactions to posts, videos and content	Social media followers, reactions, shares, comments and likes

For data brokers that specialize in selling demographic, psychographic and behavioural data, the types of data they offer can provide specific details on consumers’ interests, activities, habits and lifestyles, which are also referred to as attributes. Thus, when a B2C firm is looking to segment and target customers based on shared characteristics, behaviours and/or interests, a data broker can pull specific attributes from their data dictionary. For example, Data Axle, a Houston, Texas-based Data Broker with an office in Mississauga, Ontario, advertises “quality consumer data to power your marketing and business needs” on 11 million Canadians with over 175

¹⁰ The consumer attributes and data volume were received via email following a data sample request sent to Redmob through Datarade. Redmob’s data schema can be found here:

<https://docs.google.com/spreadsheets/d/13rDXmIwnNaTXreNdlbgU8fVOA7hQrrqRB4Pu9opyAJ4/edit#gid=0>

Redmob’s data volumes can be found here:

<https://docs.google.com/spreadsheets/d/1dExhpGHnqfahBnx5MKFFB4ybnJMdjZCEXt2wt-jD34c/edit#gid=0>

attributes (Data Axle Canada 2024). The Data Axle data dictionary contains records of these attributes spanning from interests (such as golf, liberal politics and TV movies), political party affiliation, mortgage type and vehicle make (see Image 1)¹¹. Interests are scored on a scale of 1 (low) to 9 (high) and are based on the recency, frequency, monetary value of purchases, memberships, magazine subscriptions, and survey responses (Data Axle 2024). According to Data Axle, all the company’s data is compliant with Canadian privacy laws as it is collected from either publicly available sources, such as the White Pages, from interest-based magazines or data collected through surveys conducted by research companies. To purchase a list from Data Axle, the price ranges from \$199 to \$10,000 (CAD) depending on quantity, data type and target area.

Image 1: Data Axle Data Dictionary

interests.travel Travel	Interested in traveling. Includes cruises, domestic travel, and recreational vehicles.
interests.trucks Trucks	Interested in trucks, shown through purchasing custom truck parts and/or reading truck modificati..
interests.tv_movies Tv Movies	Interested in watching and purchasing television and movies.
interests.wildlife Wildlife	Interested in the environment and/or wildlife.
interests.womens_apparel Womens Apparel	Either purchased or has shown interest in women's clothing.
interests.womens_fashion Womens Fashion	Either purchased or has shown interest in more upscale, trendy, fashionable women's clothing.
last_name Last Name	The last name of the person.
lifestyle_segment Lifestyle Segment	The lifestyle segment of the family.
location_family_count Location Family Count	The actual number of deliverable families identified at the location.
location_unit_count Location Unit Count	The actual number of deliverable units identified at the location.
mailing_score_code Mailing Score Code	The deliverability score of the location address.
mailing_street Mailing Street	The mailing address of the person or family.
middle_initial Middle Initial	The person's middle initial.
mortgage.created_at Created At	The date and time the mortgage detail was created.
mortgage.estimated_home_equity Estimated Home Equity	An estimate of the current home equity.
mortgage.estimated_interest_rate Estimated Interest Rate	The interest rate on the mortgage loan.
mortgage.estimated_loan_to_value Estimated Loan To Value	The estimated loan to value ratio.
mortgage.estimated_monthly_payment Estimated Monthly Payment	The estimated monthly payment for the mortgage.

In addition to selling data lists based on specific attributes, data brokers can also license access to their data products. In Oregon, the State defines data brokers as a “business that collects and sells or licenses brokered personal data to someone else” whereby “licensing brokered personal data is granting access to or distributing data from one person to another in exchange for consideration”, such as money (State of Oregon 2024). The inclusion of licensing is a crucial

¹¹ The Data Axle data dictionary can be found at: <https://platform.data-axle.com/people/attributes>

addition to the definition of data brokers as it highlights the different transaction models these firms use to generate revenue. Selling a list of consumer profiles is a one-time transaction whereas licensing a list can offer recurring revenue as access to the data is temporary. Licensing can also lead to increased revenues for data brokers as the data can be updated annually which justifies a higher fee compared to a one-time sale of a static list. For example, Gravy Analytics by Unacast (2024) “Audiences - interest-based targeting audiences for the U.S. and Canada built on real-world consumer visits and behavior” contains 7,000 pre-existing syndicated audiences and 2,000 leading brands and chains represented. This data can be used for advertising, audience targeting, behaviour-based audiences, audience extension, and audience creation. The starting price for this dataset is \$2 USD per CPM (or one thousand interactions), increasing to \$10,000 USD for a one-off purchase and to \$30,000 USD for a yearly license (Datarade and Gravy Analytics by Unacast 2024).¹²

In the past, the primary business model of the data broker industry was selling static lists of consumer data based on a set of specific attributes. As seen with Gravy Analytics by Unacast and RedMob this traditional data broker model still exists and continues to be profitable. However, in addition to selling original lists, data brokers can also sell data appends which are supplemental information about a firm’s existing or potential customers (Bergemann and Bonatti 2019). This involves a B2C firm granting a data broker access to their zero- and first-party data who then enriches the firm’s data with data they own.

Prior to uploading customer data to a data broker, it is imperative that firms do their due diligence. According to Calum Docherty, an associate member of the Data and Technology Transactions Practice at Latham and Watkins LLP, due diligence is “about accountability and control”, ensuring that the data is accurate and knowing what the data broker is doing with the data. With a plethora of new technologies unleashed in the digital age that can be employed to track, collect and commodify consumers’ behaviours, interests and habits, the data broker industry is evolving. For Canadians, this evolution is resulting in the widespread collection and monetization of their personal information.

Although the business practices of these traditional data brokers can be deemed invasive, widespread and largely unethical, it does not necessarily mean their business practices are illegal or contravening any of the statutes that comprise Canada’s privacy regime. If meaningful consent was given for zero-party data to be sold to a ‘third-party’, technically that transaction is permissible under PIPEDA. Issues with compliance arise when the types of personal information discussed above are collected, used, shared or sold without consent or when consent clauses are buried deep within privacy policies. The widespread collection, use and disclosure of personal information by data brokers is also a violation of PIPEDA’s Principle 4 – Limiting Collection and Principle 5 – Limiting Use, Disclosure and Retention. However, since PIPEDA is quasi-self-regulatory, outdated and has limited enforcement mechanisms, data brokers have a great deal of discretion in determining how their business practices fit within the PIPEDA framework. These issues with PIPEDA will be discussed in greater detail in Chapter 5.

Beyond PIPEDA, Canada’s patchwork privacy regime also includes provincial and industry specific laws. Provincially, there are six substantial similar statutes for personal information and personal health information. In the case of Québec’s Law 25, the privacy

¹² The Gravy Analytics by Unacast is listed on Datarade’s data marketplace under their category of consumer data.

protections are stronger. In terms of marketing and advertising practices firms and individuals must comply with the *Competition Act* and *Canada's Anti-Spam Legislation (CASL)*, both of which impose stricter penalties for noncompliance than PIPEDA. With Canada's federalist structure, a patchwork of laws and regulators will always exist. By employing a responsive regulatory approach, which expects and encourages continuous improvements for achieving better outcomes (Braithwaite 2012), the patchwork could transform into a interoperable and harmonious privacy framework that protects the personal information of Canadians from data brokers. Especially as new opportunities for data monetization and increased profits emerge.

4.2: Digital Age Data Brokers: A New Typology

In Canada, the Office of the Privacy Commissioner (2014) defines data brokers as “companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies.” While this definition provides a useful starting point for identifying the traditional data brokers discussed in the previous section it does not account for data brokers that monetize personal information beyond strictly selling or reselling. Firms that trade, share, analyze, manage and append consumer data are also data brokers, and it is through these business models that the data broker industry is expanding. Thus, a more comprehensive definition of a data broker would be “a company whose primary business involves the trading and analysis of personal information” (CIPPIC 2006). Despite fitting this definition, no actors in the data-driven ecosystem self-identify as data brokers (CIPPIC 2018a). Instead, data brokers claim to be data providers, Data-as-a-Service (DaaS) providers, marketing analytics firms or people-based marketing specialists (CIPPIC 2018a). By hiding behind these classifications, data brokers can continue their clandestine operations and avoid garnering attention from both the public and the government.

Data, like agricultural goods and metal products, is a commodity that is traded in multiple markets known as information markets. There is no single, unified market for personal data, instead, there are multiple markets in which data is traded (Acquisti, Taylor, and Wagman 2016). There are markets where data aggregators buy and sell data to other organizations, markets in which consumers exchange personal information for free products or services and markets where consumers attempt to explicitly trade their data in exchange for money (Acquisti, Taylor, and Wagman 2016). It is within these markets that data brokers, regardless of their self-identification as such, buy, sell, append, trade, manage and analyze data.

To better grasp the players that comprise the data broker industry, beyond the traditional data brokers discussed in section 4.1, I have developed a six-category typology of digital age data brokers. Enabled by technological advancements in the digital age, the firms in this typology have developed profitable business models that monetize consumer data beyond selling or licensing lists of attributes. Since the firms in this typology still profit from the collection, use, analysis, and disclosure of consumer data I consider them to be data brokers. The reasoning behind classifying these firms as data brokers is twofold. First, given the lack of knowledge about the data broker industry defining these firms as data traffickers, traders or vendors instead of data brokers would be antithetical to this dissertation's objective of calling attention to this industry. Thus, for continuity, these firms are classified as digital age data brokers. Second, this digital age data brokers typology is named to reflect the technological changes brought about by the digital age that have contributed to the advancement and growth of this industry. The six types of digital age data brokers that collect, trade, analyze, and/or manage consumer data in Canada are as follows:

AdTech Stack: AdTech or advertising technology is a complex ecosystem with tools and software advertisers use to deliver and measure digital advertising campaigns. Data management platforms (DMP) collect, organize and activate first- and third-party data from various sources to build detailed customer profiles that are then made available to ad exchanges, demand-side-platforms (DSPs) and supply-side-platforms (SSPs) to drive targeting and personalization (Oracle n.d.). DSPs are software tools that advertisers use to buy digital ads across various channels, while SSPs are tools for publishers to sell their ad inventory (Amazon Ads n.d.). DMPs typically pull data from a firm's Customer relationship management (CRM) software, which is designed to track interactions between a brand and an individual customer. In addition, firms can also employ a customer data platform (CDP) which collects, cleans and consolidates first-party data from various touchpoints such as ad clicks, website traffic and online interactions, across the entire customer lifecycle (Salesforce n.d.). Many CDPs also act as a data activation platform (DAP) by allowing firms to leverage their zero- and first-party data for advertising. For example, The Trade Desk is primarily a DSP or a programmatic advertising platform that brings advertisers and media buying agencies together to bid on ad space. However, The Trade Desk partners with many data providers, including traditional data brokers and data marketplaces, to provide a data activation service through its Galileo platform.

Big Tech and/or Platforms: Large online platforms have fundamentally altered the personal data ecosystem. Offering free and/or subscription-based products and services, online platforms such as Google, Instagram, Pinterest and Spotify collect vast amounts of personal information about their users which can be used to personalize content and deliver targeted advertisements. From demographic data to social connections to search history and shopping habits, this data is used to create detailed profiles that are the basis of personalization and targeted advertising. Unlike traditional data brokers, these platforms do not sell or license their data products. Instead, advertisers specify their target audiences and for a fee, the platforms, such as Facebook, match user profiles with relevant ads. The target audience can be a custom audience intended to target a specific group or a lookalike audience which entails creating a new audience based on the characteristics of existing customers. Google similarly monetizes user data. By building individual profiles based on demographics and interests, Google permits advertisers to target specific groups or by selling ad space through real-time bidding which entails sharing sensitive user data such as device IDs, cookies and browsing history with ad tech companies (Cyphers 2020). Despite Meta and Google both stating they will never sell any personal information to third parties, in 2023 the two platforms generated \$131 billion (USD) and \$237 billion (USD), respectively, in advertising revenue from monetizing user data (Alphabet Inc. 2024; Meta Platforms, Inc. 2024).

Data Marketplaces: Data marketplaces are online stores that connect data providers and data consumers, offering participants the opportunity to buy and sell data. As many businesses seek to enrich or monetize their first-party data, data marketplaces offer an efficient one-stop-shop where interested buyers can browse, sample and purchase various data products from numerous sellers across a range of industries. Proprietary marketplaces such as Snowflake, AWS Data Exchange and Oracle Data Marketplace operate their enclosed platforms making it convenient for data to be exchanged with users across the platform (Databricks 2023). There are also public data marketplaces, such as Datarade, which are accessible to any firm or individual looking to either purchase or sell data. The price for the data products depends on the platform, the amount of data being exchanged and whether it is a one-time purchase or a license. While data marketplaces are

not directly buying or selling zero, first or third-party data these firms are facilitating and profiting off the sale of consumer data.

Loyalty Programs and Rewards Credit Cards: Advertised as saving consumers money through rewards programs and membership discounts, loyalty programs primarily serve as a valuable tool for collecting consumer data. By tracking purchases, behaviours and preferences, loyalty programs generate valuable insights on consumers that can then be used to increase profits. Loyalty programs collect demographic, analyze shopping patterns, record transactions and track customer interactions all of which are used for targeted advertising, customer segmentation and serving personalized shopping recommendations. The largest loyalty programs in Canada include SPC Card (Student Price Card), PC Optimum, Aeroplan, Triangle Rewards (Canadian Tire) and Plum (Chapters-Indigo). According to a marketing executive, loyalty programs allow advertisers to market to their user base, for a fee, without ever seeing the data. This involves serving advertisements in the background to specific groups. The same applies to rewards credit cards such as the Scotiabank Scene+ Visa card, CIBC Aeroplan Visa Infinite card and the Presidents Choice Financial World Elite Mastercard. With these credit cards, the rewards partners (i.e. Scene, Aeroplan and Presidents Choice) can access the shopping habits of all cardholders that they would otherwise not be able to see. The use of data collected from loyalty programs and rewards credit cards to serve and sell targeted advertisements and promotions results in the categorization of these firms as digital-age data brokers.

Market Research Companies: Market research involves gathering information about market needs and preferences to help other firms understand their target market (Qualtrics n.d.). By analyzing data collected through interviews, surveys, focus groups and social listening, market research companies offer businesses valuable insights into industry trends, consumer preferences and competition (Brandwatch 2023). In addition to this primary research, these companies can also provide data collected through industry reports, public databases and other companies' proprietary data, also known as secondary research (Cote 2022). Using a combination of survey and census data, Environics PRIZM "features 67 segments that capture current demographics, lifestyles and values in Canada... that gives you access to over 40,000 data points and can be combined with your own customer data" (Environics n.d.). Some of the other largest market research companies are Ipsos, Qualtrics and, Nielsen. Market research companies monetize the data they collect by offering consulting services, selling research reports and/or licensing their data. Since these companies collect, analyze and sell consumer data insights for profits, despite respondents consenting to participate, they are included in this typology.

Media Buying Networks: Media buying is the process of purchasing traditional (broadcast television and newspapers) and digital (social media and websites) advertisement space for marketing campaigns (Shopify 2023). More specifically, media buying involves securing the ideal location, placement and times to run ads that are most relevant to the brand's specific audience and achieve the lowest cost per action (Amazon Ads n.d.). Media buying networks are firms that specialize in buying and selling advertisements. These networks often act as intermediaries between firms looking to advertise and media outlets or advertising channels. To optimize ad placements and campaign performance media buying networks create user profiles and target audiences for advertising campaigns by collecting and analyzing consumer data. Media buying networks can obtain consumer data via data partnerships with third parties, such as traditional data

brokers and DMPs, data marketplaces and/or directly from their clients. For example, illumin (formerly acuity ads) is the only journey advertising platform that brings media planning and buying together. illumin also partners with various traditional data brokers and market research companies including eXelate by Nielsen, Lotame and LiveRamp to acquire consumer data. Moreover, according to a former illumin employee “some clients keep their contact lists private, others don’t. For the clients that share access to their customers’ data, it provides illumin with a large database of consumer data that you have to assume they are re-using or re-selling.”¹³ Since media buying networks are not directly selling consumer data but are instead profiting off the collection and use of consumer data to maximize advertising campaigns, these firms are considered digital age data brokers.

Across the digital age data broker typology, the distinctions between the six types of firms are not stark. Instead, they are blurry as many firms provide products, services and solutions that fit into multiple categories. For example, The Weather Network, owned by Oakville, ON based Pelmorex Corporation, does not exclusively provide customized location specific weather information to app or online users. Instead, as a free service Pelmorex generates revenues by selling the aggregated and anonymized data of The Weather Network users (Pelmorex Corp n.d.). More specifically, Pelmorex offers location data received from over 16.9M devices and collected from a variety of additional premium data partners, data on users behaviours, demographics and purchases as well as private marketplaces (Pelmorex Corp n.d.). Therefore, in addition to being a Big Tech/Platform, Pelmorex and The Weather Network also fall under the AdTech, Media Buying Network, and Marketplace categories as well as being a Traditional data broker.

With digital age data brokers falling into multiple categories based on their various business practices consumers and regulators would have a difficult time discerning which firms are monetizing their data and through what practices. The Weather Network highlights these challenges. Now more than ever it is imperative for consumers to be more cautious when clicking through a pop-up cookie banner and making the decision to disclose or protect their personal information. The new reality for the data broker industry is that firms are no longer simply selling static lists or licensing access to their data products. Instead, the firms in this typology also face a trade-off of sharing and protecting their data. As the data broker industry continues to evolve and becomes increasingly complex regulators must also adapt and be responsive to the technological changes that are enabling new data harvesting tools and data monetization techniques. Even with limited powers, it is necessary for privacy regulators to utilize the investigative and enforcement tools at their disposal to identify the ways in which these firms are collecting and monetizing consumer data in noncompliant manners.

As seen with the business practices of the digital age data brokers, firms participating in information markets are monetizing their data without relinquishing their data. DSPs, Big Tech platforms, loyalty programs, rewards credit cards and media buying networks can segment out and serve ads to specific audiences without giving a partner or client firm access to their proprietary data. The lack of transparency and visibility into the data being used for targeted advertising coupled with the success of the firms in this typology speaks to both the quality and quantity of the data these firms possess. As new and existing firms develop more pervasive and effective ways

¹³ Interview with former employee of illumin (formerly Acuity Ads) conducted on April 7th, 2024

to monetize consumer data without strictly selling access to the list, identifying the key players that comprise the data broker industry will become increasingly complex.

Additionally, as the data harvesting and acquisition techniques of digital age data brokers become increasingly technical both consumers and regulators will have less knowledge on how personal information is being used or if meaningful consent was obtained. Consequently, the complexity and opaqueness of both traditional and digital age data brokers will ensure the industry remains under-regulated as neither consumers nor regulators will be able to determine if and how these business practices violate Canadian privacy laws. Since digital age data brokers do not self-identify as data brokers it will be increasingly difficult for regulators to determine the size and scope of the industry, especially as technological advancements create new data monetization business models, and thus, new subcategories of digital age data brokers. This will further exacerbate the under regulation of the global data broker industry in Canada.

4.3: The Global Data Broker Industry in Canada

With over 500, 300 and 100 data brokers respectively registered in California, Texas and Vermont (California Privacy Protection Agency 2024; Office of the Vermont Attorney General 2019; Texas Secretary of State 2024), the size and scale of the data broker industry in the U.S. is slowly being revealed. For consumers this increased transparency can help consumer understand what entities are collecting their data and how to opt-out of data collection. For state level policymakers these registries can assist with creating industry specific enforcement strategies that offer consumers additional privacy protections. In contrast, there are no national or sub-national data broker registries in Canada that can shed light on the industry's size and business practices. To increase awareness around the firms monetizing Canadian consumer data, this section presents a list of over 150 data brokers operating in Canada. In doing so, this section aims to increase the transparency around the global data broker industry's operation in Canada and discuss the challenges as well as solutions for regulating a complex, clandestine and global industry.

The Data Brokers in Canada list, found in Appendix A, identifies 152 traditional and digital age data brokers that monetize Canadian consumer data. The list includes the firm name, type of data broker and a link to their website. Regarding the type of data broker, the list identifies firms as traditional, specifying the type of data they monetize, or based on the firm's classification under the digital age data broker typology. If the business practices of a data broker fall under multiple categories, they are listed. For example, LiveRamp is listed as traditional, marketplace and AdTech. Additionally, the list also specifies what type of information the traditional data brokers specialize in monetizing (i.e., location, attributes or B2B). What this is does not include are any B2C e-commerce firms or retailers that monetize their customers data or purchase data about their customers. Since these firms typically partner with data brokers to increase their revenues via targeted advertising and personalized offerings but do not monetize customer data as a primary revenue stream, they are not considered data brokers and are thus excluded. However, B2C firms with loyalty or rewards programs such as Air Canada's Aeroplan or Marriott Bonvoy are included.

With the Data Brokers in Canada list, it is possible to evaluate the global data broker industry in Canada and determine the number of traditional versus digital age data brokers that are monetizing the personal information of Canadians. Of the 152 identified data brokers, 28 firms are categorized exclusively as traditional data brokers, meaning they collect, purchase, sell and/or license lists of attributes, locations, behaviours, health data and financial information. Some

examples of these firms include Acxiom, Data Axle, Equifax, Reklam¹⁴ and TransUnion. Including these 28 firms, there are 76 data brokers in total that can be categorized as both traditional and digital age data brokers. Firms such as 33Across, LiveRamp and Numeris offer a combination of products and services that lead them to be categorized under traditional, AdTech stack, marketplaces and market research firms.

For the digital age data brokers specifically, there are 83 data brokers that fall under the AdTech stack category. However, of this 83 only 14 are exclusively AdTech firms, the remaining 69 data brokers can be categorized as AdTech and Marketplace, AdTech and Media Buying Network or AdTech and Big Tech/Platform. Turning to Big Tech/Platforms firms, there are 14 identified on the Data Brokers in Canada List including Amazon, Meta, Pinterest and X. In addition to these digital age data brokers, there are 12 firms listed that can be classified under Loyalty Program and Rewards Credit Card. These firms include Airmiles, Cineplex and Scotiabank (for the Scene+ program) Metro's Moi program and Hilton Honours. Lastly, there are 11 media buying networks, such as Loblaw Advance, and 10 market research firms, such as Ipsos and Numeris, on the list.

With varying business practices and data monetization techniques there is a complex array of traditional and digital age data brokers operating in Canada, many of which are not Canadian firms. Of the 152 data brokers, 37 are headquartered in Canada, 98 are American based and the remaining 17 are from Europe and Asia. The strong presence of American compared to European or Asian data brokers in Canada can be attributed to the close geographic and economic ties between Canada and the U.S., the presence of Silicon Valley in California (which is where many data brokers are located), and the similarities between Canadian and American consumers. Large data brokers, such as TransUnion, Equifax and Data Axle, not only operate in Canada but also have physical offices and branches, a practice not typically followed by smaller firms whose services can be provided remotely. In terms of privacy, having a physical presence in Canada can assist these American firms in complying with PIPEDA or the provincial statutes by storing personal information in Canada.¹⁵ However, with digitalization and globalization enabling transborder flows of personal information, cross-border data flows and e-commerce are now integral to digital trade and the data-driven economy.

For states and firms, promoting cross-border data flows and eliminating barriers digital trade have become a priority. As discussed in Chapter 2, at the international level, the WTO has recognized the implications of digitalization for trade but has yet to implement any rules or agreements that govern digital trade. To fill the gap left by the WTO and encourage the growth of the data-driven economy, states have included digital trade, e-commerce, privacy, and cross-border data flows provisions in their FTAs and PTAs. Following in the footsteps of the U.S., Canada's approach to supporting international digital trade is mainly based on trade agreements (Leblond 2022).

¹⁴ Reklam (Reklam n.d.) is a platform that enables consumers to take control of their digital identity. The platform allows individuals to access their data, see how many companies are buying their data and sell their data to brands for points which can be reclaimed for money via PayPal or Venmo or for gift cards.

¹⁵ By storing Canadian data in Canada, American firms can eliminate the need for implementing additional safeguards to transfer the data internationally and thus, simplify their compliance cross-border data transfer rules and regulations set out by PIPEDA and the provincial statutes.

The 2008 Canada–Peru FTA, 2008 Canada–Colombia FTA, 2013 Canada–Honduras FTA, 2013 Canada–Panama FTA, and 2014 Canada–Korea FTA all contain non-binding provisions that aim to enable e-commerce and cross-border data flows (Burri and Polanco 2020). For example, the Canada–Korea FTA states the Parties affirm the importance of maintaining cross-border flows of information as an essential element in fostering a vibrant environment for electronic commerce (Article 13.7(c)). The Canada–Peru FTA (Article 1508(c)) and Canada–Honduras FTA (Article 16.5(c)) both contain provisions with similar wording. These agreements have materialized in response to the WTO recognizing the implications of digitalization for trade but failing to keep up with the data-driven economy by establishing rules to govern digital trade (Aaronson and Leblond 2018). In addition to bilateral FTAs, regional FTAs are also used to govern cross-border data flows and e-commerce.

The Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP) is comprised of 10 parties that have agreed to a set of rules facilitating economic growth through the use of the Internet and preventing barriers to digital trade (Peng 2023) and the Canada–United States–Mexico Agreement (CUSMA) incorporates new articles to address 21st-century trade issues. Chapter 14 of the CPTPP, *Electronic Commerce*, and Chapter 19 of the CUSMA, *Digital Trade*, contain identical provisions to foster digital trade, e-commerce, and cross-border data flows. Despite some minor differences in the word of the provisions, the CPTPP and the CUSMA both promote and encourage cross-border flows of information. Article 14.11.2 of the CPTPP states “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” whereas Article 19.11.1 of the CUSMA stipulates “no Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.” To further eliminate barriers to trade and foster innovation, the CPTPP and the CUSMA both encourage self-regulation. CPTPP Article 14.15(e) and CUSMA Article 19.14(d) both state Parties shall endeavour to “encourage development by the private sector of methods of self-regulation that foster digital trade, including codes of conduct, model contracts, guidelines, and enforcement mechanisms.”

Since eliminating trade barriers, and not protecting privacy, is the primary goal of an FTA, the scales are tipped in favour of trade instead of privacy. The promotion of cross-border data transfers and self-regulation stipulated in the CPTPP and the CUSMA benefits the data broker industry and its operation in Canada in two ways. First, the free flow of information across borders opens new markets for data brokers. In doing so, the FTAs not only allow but encourage data brokers to transfer, store and sell Canadian consumer data outside of Canada. Second, with the FTAs encouraging the self-regulation of the private sector, the data broker industry in Canada, which is already quasi-self-regulating, has been left to grow with minimal government interference.

For individuals, these barriers to trade and cross-border data flows are the privacy laws and regulations that aim to protect their personal information. Canada’s patchwork privacy regime, which is discussed at length in Chapter 5, not only fails to prevent data brokers from monetizing personal information but enables their business practices. Due to PIPEDA non-prescriptive and principle-based nature, firms such as data brokers, are afforded a great deal of discretion in

outlining the purposes for collecting and using data. Additionally, while PIPEDA governs international data transfers, the ability of the Canada's privacy Commissioner to enforce the Act both at home and abroad is rather limited. Conversely, the EU's General Data Protection Regulation (GDPR), seen globally as the gold standard of privacy protection, offers European consumer more stringent privacy protections.

The GDPR fundamentally altered the digital economy and the way companies across the globe collect, store, and use personal data, both of which demonstrate the global reach of the Brussels Effect (A. Bradford 2019).¹⁶ In terms of cross-border data transfers, the GDPR and PIPEDA are notably different in several respects. First, PIPEDA places the onus of ensuring comparable protection on organizations carrying out data transfers (Schedule 1 s. 4.1.3) whereas the GDPR places that onus on both the exporter and recipient organizations (Article 46). Second, the GDPR expressly requires data processors to carry out a Data Privacy Impact Assessment ('DPIA') in certain circumstances (Article 35), while PIPEDA does not establish Privacy Impact Assessment ('PIA') requirement. Third, data controllers outside the EU involved in certain forms of processing are obligated to designate a representative based within the EU (Article 27). PIPEDA does not require organizations outside of Canada to designate a representative in Canada (Schedule 1 s. 4.1 and 4.2). Lastly, under the GDPR, transfers of personal data to non-EEA (European Economic Area) countries may take place on the basis of an adequacy decision (Article 45) or appropriate safeguards (European Data Protection Board n.d.). If the European Commission determines that a non-EEA country offers an adequate level of data protection, personal data can be transferred to organizations in that country without additional safeguards (European Data Protection Board n.d.). With PIPEDA there are no specific provisions for cross-border data flows. Instead, the Act states that organizations are responsible for personal information that has been transferred to a third party for processing.¹⁷

When personal information crosses borders, it becomes subject to a variety of legal frameworks which raises concerns as to whether the level of protection in a foreign jurisdiction is sufficient. These concerns are exacerbated by the existence of data havens, which are jurisdictions with minimal to no data protection laws. In the absence of adequacy requirements similar to GDPR Article 45, firms may transfer data to these jurisdictions to evade stringent regulations when processing personal information. These transfers can lead to various misuses of personal information arising from unauthorized access, data breaches and state surveillance. In February 2024, U.S. President Joe Biden issued an executive order restricting "access by countries of concern to Americans' bulk sensitive personal data and U.S. Government-related data" that can be used to track and build profiles on American individuals, including Federal employees and contractors, for illicit purposes, including blackmail and espionage (Biden 2024). However, since the U.S. does not have a federal private sector privacy law, the same data protected under the Executive Order can be freely collected, processed and sold across borders to any country or firm that is not deemed a foreign adversary.

¹⁶ Anu Bradford's (2019). Brussels Effect describes the European Union's unilateral regulatory power and its ability to establish global regulatory rules in a range of including privacy, antitrust and food safety.

¹⁷ Under Québec's *An Act to modernize legislative provisions as regards the protection of personal information*, public bodies are required to conduct a privacy impact assessment prior to releasing personal information outside the province (s 70.1) (National Assembly of Québec 2021).

The global nature of the data broker industry, the promotion of cross-border data transfers in FTAs and Canada's weak privacy regime have created a favourable environment for these firms to collect, process and monetize Canadian consumer data regardless of their location. Together, these three factors contribute to the under-regulated data broker industry in Canada. With a mix of firms that use varying data monetization practices, operate outside of Canada and do not identify as data brokers, it would be extremely challenging for policymakers to effectively regulate an industry in which the size, scale and scope is unknown. Factoring in FTAs with provisions that are antithetical to protecting privacy, regulators face additional challenges as the business practices of data brokers are promoted and encouraged in provisions on digital trade and cross-border data flows. The strong presence of American data brokers operating in Canada also contributes to the under regulation of this industry as the OPC's weak and complaint-based enforcement system is unable to adequately safeguard the cross-border flow of Canadian consumer data.

To address the issues discussed across this section and effectively regulate the business practices of the global data broker industry in Canada a responsive regulatory approach should be taken. Given the large number of American data brokers in Canada and the weak protections for cross-border data flows, it would be beneficial for a Canadian data broker registry to be created. To do so, the OPC should collaborate with the provincial privacy commissioners as engaging a wider network of partners is promoted under responsive regulations as it increases the pressure on the regulated entities and thus, the chances of compliance (Braithwaite 2012). With this registry, the OPC can then start to identify and differentiate between data brokers based on their business practices. In doing so, the OPC can be responsive to the ways in which the subsets of data brokers violate privacy and to their evolving data monetization techniques. Additionally, with the registry the OPC can start to determine the true size and scope of the data broker industry and its operation in Canada.

Concluding Remarks

According to a 2018 study, the global data broker industry is comprised of thousands of companies generating some US\$200 billion in annual revenue (Crain 2018). With demographic data estimated to be worth 0.0005 per person and psychographic data worth at least \$0.0021 per person (Rostow 2017), the data collected and monetized by traditional and digital age data brokers is profitable if done at scale. Together, globalization, digitalization and economic liberalization have been the main drivers behind data brokers achieving this scale. For example, media buying networks, AdTech companies and data marketplaces have all become lucrative businesses by seizing new economic opportunities arising from increased access to information without government interference. Coinciding with the development of new technologies, platforms and retailers that encourage consumers to disclose their data will be new methods and firms harvesting, processing and monetizing personal information. For states pursuing profits, digital trade and economic growth, existing and emerging data-driven industries will be left to innovate and grow unencumbered by regulation.

With social media, connected devices, targeted advertising and personalized services, the data broker industry has been able to grow from firms such as Acxiom and Oracle selling static lists of consumer data to the multifaceted industry it is today. The 152 traditional and digital age data brokers identified on the Data Broker in Canada list points to the true size and scale of this industry. As new methods for data harvesting and processing emerge and more data brokers enter

the Canadian market, this list will inevitably grow. With limited transparency, highly technical data harvesting techniques and a privacy framework that prioritized profits over privacy, the challenge for both consumers and regulators will be identifying privacy violations when they inevitably occur. While the playing field between firms and consumers will never be level, employing a responsive regulatory approach can assist in tilting the scales more in favour of protecting privacy. By being adaptive to changing data monetization practices, utilizing enforcement pyramids and relying on punishment and persuasion to encourage compliance, Canadian regulators can protect privacy without banning commercial uses of personal information.

This chapter sought to provide a comprehensive overview of the global data broker industry and its operation in Canada. Through the novel contributions of the digital age data broker typology and the Data Brokers in Canada list, this chapter aims to expose and call attention to the clandestine business practices of the firms that comprise this industry. By outlining the ways in which both traditional and digital-age data brokers collect, exchange and monetize data, this chapter sets the foundation for the analysis of Canada's patchwork privacy regime (Chapter 5) and the examination into the ways in which these firms exercise their power to shape regulations (Chapter 6).

A secondary objective of this chapter is to inform both consumers and regulators on the types of firms that are monetizing personal information. With this knowledge, I hope to minimize the information asymmetries between consumers and data brokers and help Canadians make more informed decisions before disclosing their personal information, accepting all cookies or signing up for a loyalty program. The objective is not to dismantle the data broker industry or prevent digital trade. Instead, with this chapter and dissertation, I seek to give consumers a better understanding of how their personal information is collected and monetized by the firms they interact with daily. Both directly and indirectly.

Chapter 5: Privacy Protections in Canada: A Perilous Paradox

Introduction

The complexity of Canada's patchwork is not only daunting to the policy analyst, it also creates a significant and increasing set of transaction costs for businesses that operate in different jurisdictions. It is principally for these reasons that the privacy protection issue has risen to the political agenda, and that the rhetoric about 'marketplace rules-of-the-road' and 'level playing fields' on the information highway has overshadowed the traditional discourse about human rights and civil liberties within which privacy protection originated (Bennett 1996, p. 483).

Nearly 20 years after Colin Bennett's article was published, Canada's privacy landscape remains virtually unchanged. With the egregious misuse of personal information emerging alongside the promises of economic growth tied to AI, machine learning and Big Data, existing and proposed private sector privacy laws attempt to balance privacy and innovation. However, as this chapter seeks to demonstrate, the privacy regime in Canada is not balanced as innovation and industry are prioritized over privacy and justice.

Privacy, or the right to be let alone, has come under siege with the proliferation of web-connected ICT devices has led to vast amounts of personal information being collected, harvested, analyzed, and utilized by businesses, organizations and governments. From Flo, a fertility tracking app, sending user's health information to Facebook without consent (Schmunk 2024) to Tim Horton's tracking the geolocation of its app users' anywhere in the world, even when the app was closed (Austen 2022), to the RCMP's use of Babel Street, a threat intelligence tool, to source and collect publicly available information and social media accounts (Boutilier 2024), any information posted online or shared via a platform is easily repurposed or commodified. Despite the Supreme Court of Canada's long-standing interpretation of privacy law as having quasi-constitutional status and international legal instruments such as the United Nations 1948 Universal Declaration of Human Rights (UDHR) having recognized the fundamental right to privacy (Dufresne 2023), Canadians continue to have limited protections that permit them to control, access, update or delete their data.

To advance the central argument of this dissertation, this chapter identifies and critically examines three key aspects of Canada's privacy regime that either fail to adequately safeguard the privacy of Canadians or encourage the collection and monetization of personal information by data brokers. The three dimensions I identified are as follows: a complex patchwork of privacy statutes, the reliance on firms to quasi self-regulate and the weak enforcement powers of the Office of the Privacy Commissioner. With this chapter, I seek to explain that given Canada's weak privacy regime the business practices of data brokers can be deemed either compliant or partially compliant as profits have been prioritized ahead of privacy.

The chapter is organized as follows. Section 6.1 overviews the statutes that comprise Canada's patchwork privacy regime to illustrate the complexity of these laws and the subsequent consequences for firms and Canadians. Section 6.2 presents the self-regulatory aspects of Canadian privacy laws and how firms can exploit this freedom and flexibility to justify their privacy violating business practices as compliant. Section 6.3 discusses the weak enforcement powers of the Office of the Privacy Commissioner under both PIPEDA and the *Consumer Privacy Protection Act* (CPPA) and how the ombuds model is no longer equipped to address privacy violations in the age of Big Data.

5.1 Canada's Patchwork Privacy Regime

Privacy protections in Canada operate within a complex legal framework that attempts to safeguard personal information while balancing federalism, public versus private sectors, and economic growth. To safeguard personal information, the primary privacy and data protection laws in Canada are statutory (Penney 2022). Arising from concerns about the use of computers for processing protection of personal information by the government, Canada enacted its first federal public sector privacy protection in 1978 under Part IV of the *Canadian Human Rights Act* (Savoie et al. 2020). This provision granted individuals the right to correct, limit access to and control the dissemination of their personal information held by federal government institutions (Hayward 1984). In 1983 Government of Canada would remove privacy protections from the Human Rights Act and enacted Bill C-43 which would introduce the *Privacy Act* and *Access to Information Act* (Savoie et al. 2020).

The *Privacy Act* protects “the privacy of individuals with respect to personal information about themselves held by a government institution” (Privacy Act, 1983, s.2). The Act applies to the collection, use and disclosure of personal information by the Government in the course of providing old age security pension, employment insurance, border security, federal policing, tax collection and public safety (Office of the Privacy Commissioner of Canada 2018c). In Section 3 of the Act, personal information is defined as any recorded information about an identifiable individual including their age, race, marital status, education, fingerprints, blood type and address. The *Privacy Act* grants Canadian citizens and permanent residents the right to access their information and request a correction if there are errors or omissions (s. 12(1)(2)). If an individual suspects their information has been used or disclosed in a manner that contravenes the Act, sections 29 – 31 allow a complaint to be filed with the Office of the Privacy Commissioner of Canada (OPC) who can then investigate (Office of the Privacy Commissioner of Canada 2018d).

The *Personal Information Protection and Electronic Documents Act* S.C. 2000, commonly abbreviated to PIPEDA, applies to the collection, use, disclosure and cross-border transfer of personal information by private-sector organizations (Office of the Privacy Commissioner of Canada 2018b) ¹⁸. More specifically, PIPEDA seeks to establish “rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances”(Part 1, s.3). The backbone of PIPEDA is the 10 Fair Information Principles (FIPs) outlined in Section 5 and Schedule 1 of the Act include accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance. These principles hold organizations responsible for the protection and fair handling of personal information both internally and in dealings with third parties (Savoie et al. 2020). If an organization contravenes PIPEDA, the OPC has the power to receive or initiate complaints, investigate, and attempt to resolve complaints (s. 11 – 12), audit organizations (section 18) and publicize the information practices of an organization (s.20).

In the absence of significant updates, PIPEDA is becoming increasingly inadequate for safeguarding personal information in the digital age. In response to the emerging signs of

¹⁸ Despite receiving Royal Assent in 2000, PIPEDA did not apply to personal information used by the health sector until 2002 and to all private sector organizations until 2004. (Levin and Nicholson 2005).

obsolescence, the federal government has sought to update Canada's privacy regime. In November 2020, the Liberal government introduced Bill C-11 *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts* which would repeal and replace parts of PIPEDA. However, this bill died on the Order Paper when Parliament was dissolved on August 15th, 2021, in advance of the federal election. In June 2022, the government reintroduced *The Digital Charter Implementation Act* in Bill C-27 which includes three statutes: the *Consumer Privacy Protection Act* (CPPA), the *Personal Information and Data Protection Tribunal Act* and the *Artificial Intelligence and Data Act* (AIDA). Under the CPPA organizations would be required to implement and maintain a privacy management program and the OPC would have powers to issue compliance orders (s.93(2)) as well as grant a private right of action for damages (s. 107(1) (2)).

In addition to these privacy-enhancing features of Bill-C27, there are also several clauses, provisions and definitions in the CPPA that undermine privacy. First, the CPPA includes a legitimate interest clause which stipulates that an organization “may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use” (s. 18(3)). Second, the CPPA in determining whether an organization must use implied or expressed consent, the sensitivity of the information must be considered (s. 15(5)) (Scassa, 2022). Thus, for any information not deemed sensitive firms can rely on implied consent for the collection, use and disclosure of that information. Lastly, Bill C-27 does not define sensitive information or high-impact AI systems, include a section on international data transfers, outline the degree of granularity required for plain language in privacy policies or recognize Indigenous data sovereignty.

Indigenous data sovereignty “describes the fundamental rights of Indigenous Peoples' to control, access, interpret, manage, and collectively own data about their communities, lands, and cultures” (Mukunda 2024). For Indigenous Peoples', data sovereignty is central to overcoming colonial legacies and power imbalances that have resulted in their data being collected, used disclosed without their consent as well as for purposes that do not serve their communities. According to Kristin Kozar a member of the Hwilitsum First Nation, the Canadian federal government has used the data it holds on Indigenous peoples, including health, census, and Residential School records, which communities often lack access, to perpetuate anti-Indigenous stereotypes, justify colonial policies, and maintain oppression (Kozar in Laboucan 2024). The failure of the federal government to meaningfully consult with Indigenous Peoples and recognize Indigenous data sovereignty is inconsistent with the government's obligation to implement the *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP) and is inexcusable in light of the First Nations Principles of OCAP® (Centre for Digital Rights 2023).

Between June 2022 and May 2024, Bill C-27 passed a first and second reading in Parliament and was being studied by the House of Commons Standing Committee on Industry and Technology (INDU). On May 29, 2024, the INDU paused its study of Bill C-27 until September 2024. On September 23, 2024, the committee unanimously agreed to extend the pause on its clause-by-clause study until October 21, 2024 (Standing Committee on Industry and Technology 2024a). With no consensus on several aspects of Bill C-27 combined with the lack of cooperation from Minister François-Philippe Champagne in terms of providing tangible amendments to the

bill, the committee agreed on November 21st, 2024 to delay its study of Bill C-27 until 2025 (Standing Committee on Industry and Technology 2024). However, when Prime Minister Justin Trudeau prorogued Parliament on January 6th, 2025, the INDU’s study of Bill C-27 was terminated. With the ending of the 44th Parliamentary session, the Digital Charter Implementation Act, 2022 died on the Order Paper for a second time.

In Canada, personal information is also regulated under provincial privacy laws, adding another layer to Canada’s privacy patchwork. Alberta, British Columbia, and Québec have enacted laws that govern the collection, use and disclosure of personal information by private sector organizations and New Brunswick, Newfoundland and Labrador, Nova Scotia and Ontario have adopted laws to govern personal health information (see Table 3). These provincial private sector and personal health information privacy laws have been deemed ‘substantially similar’ to PIPEDA. This means that in many circumstances, the provincial law applies instead of the federal law. In the provinces with health information privacy laws, both federal and provincial legislation may apply as their statutes have been deemed substantially similar to PIPEDA with respect to ‘health information custodians’(Gratton et al. 2020). To be deemed substantially similar to PIPEDA, a provincial privacy statute must provide equal privacy protections; contain the 10 fair information principles; provide an independent oversight body with the power to investigate; and allow for the collection, use and disclosure of personal information for appropriate or legitimate purposes. (Office of the Privacy Commissioner of Canada 2020).

Table 3: Provincial Privacy Laws

Province	Law	Came Into Force
Alberta	Personal Information Protection Act	2004
British Columbia	<i>Personal Information Protection Act</i>	2004
Québec	Law 25 - An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information	2021
New Brunswick	Personal Health Information Privacy and Access Act	2009
Newfoundland and Labrador	The Personal Health Information Act	2011
Nova Scotia	Personal Health Information Act	2013
Ontario	Personal Health Information Protection Act	2004

In addition to the statutes discussed above, industry-specific laws and regulations are the final pieces of Canada’s privacy regime. Due to Canada’s federalist structure, there are provincial and federal acts that afford some additional protections around the use and disclosure of personal information. For consumer credit reporting, PIPEDA still applies, however, most provinces have legislation outlining the practices that must be adopted by credit reporting agencies (CRA) and the users of consumer credit information (TransUnion n.d.). For example, The Ontario *Consumer Reporting Act* R.S.O 1990, regulates CRAs, such as Equifax and TransUnion, who provide credit and personal information about consumers (e.g., borrowing and bill-paying habits) to third parties (e.g., insurers, employers and landlords) (Ministry Public and Business Service Delivery 2021). Under section 1(1) of the Act, credit information includes a consumer’s name, age, occupation, marital status, place of employment, estimated income, debt obligations and assets. Personal information (s.1(1)) means “information other than credit information about a consumer’s character,

reputation, health, physical or personal characteristics or mode of living or about any other matter concerning the consumer.” If any of this information is inaccurate or incomplete, section 13(1) of the Act gives consumers the right to dispute any errors and section 10 (5) restricts creditors from sharing personal information with third parties or CRAs unless consent was obtained at the time of the application. If an individual contravenes any provision of this Act and is found guilty, they are liable under section 23(1) to a fine of no more than \$50,000, one-year imprisonment or both and liable to the consumer for damages under section 21.1(1). For corporations, the maximum penalty under section 23(2) is \$250,000. Additionally, section 23.1(2) Act allows for a consumer right of action for damages.

To ensure consumer protection and responsible communication practices for marketing and advertising Canada's Anti-Spam Legislation (CASL) and the *Competition Act* come into play. Enacted in 2014, CASL reinforces best practices in email marketing and combat unwanted electronic communications such as spam. In general, CASL prohibits firms from sending commercial electronic messages (such as email, social media and text) without consent, harvesting electronic addresses and collecting personal information by accessing a computer system or electronic device illegally. The legislation mandates an opt-in consent regime, placing the onus on the sender to clearly explain the terms and the purpose of consent and, obtaining this consent must be done in addition to consent under privacy legislation (Gratton et al. 2020). For violations, CASL empowers the Canadian Radio-television and Telecommunications Commission (CRTC), the Competition Bureau, and the OPC to enforce its provisions and levy monetary penalties.

The *Competition Act*, R.S.C., 1985, enforced by the Competition Bureau, contains civil and criminal provisions for misleading advertising practices. Civilly, section 74.01(1)(a) prohibits representations to the public, to promote a product or any business interest, that is false or misleading in a material respect. Section 52(1), the general criminal misleading advertising provision is substantially similar to section 74.01(1)(a) but requires intention for making false or misleading claims. Under the civil regime, administrative monetary penalties for first occurrences are up to \$750,000 for individuals and \$10,000,000 for corporations and for subsequent occurrences, the penalties increase to a maximum of \$1,000,000 and \$15,0000 respectively (Competition Bureau 2022). Under the criminal regime, if an individual is found guilty they can be liable for a of up to \$200,000 and/or imprisonment for up to one year (Competition Bureau 2022). Regarding privacy, the Competition Bureau asserts that firms should assume consumers will be influenced by their representations about how personal information is processed and, therefore, must ensure they do not mislead consumers about the collection and use of personal information (Pennington and Wasser 2020).

For businesses operating in different provinces, the transaction costs of having to deal with different privacy laws and regulations can create uncertainty and confusion, especially for provincially regulated industries. (Bennett 1996). Thus, organizations must consider how to develop a privacy program around numerous laws that could be substantially similar yet contain different requirements in similar situations (Rostama and Scassa 2023). With Québec's Law 25 as the most stringent privacy law in Canada, both federally and provincially, there are concerns about the lack of harmonization with Bill C-27.

Testimony to the House of Commons Standing Committee on Industry and Technology (INDU) for their study of Bill C-27 highlights the concerns about interoperability and harmonization. Former President of the Commission d'accès à l'information du Québec Diane Poitras (2023) stated “there will be situations where a business will have to comply with both the rules of Bill 25 and...Bill C-27, if it's passed. It can certainly be difficult to comply with two sets of rules if the rules aren't similar. In addition, human beings being what they are, there may be a tendency to want to comply with the least restrictive rule.” According to Michael McEvoy (2023) Information and Privacy Commissioner of British Columbia since “data most often knows no borders” it is imperative for privacy regulators to act, to the greatest extent permitted by law, in a coordinated manner “to ensure that concerned individuals are addressed in a consistent way and that affected businesses are not queried by overlapping demands.” Over the past several years it has become increasingly common for the OPC and provincial privacy commissioners to collaborate on investigations pertaining to high-profile and high-impact data protection issues with national dimensions (Rostama and Scassa 2023).

Even with this collaboration, there are still issues with imbalances across the privacy laws. According to Colin Bennett’s (2023) testimony during the study of Bill C-27, if there are certain areas in Québec’s law where businesses would be required to do more than they would under the current text of Bill C-27, you have to ask: “What might be the economic impact of that across Canada if the CPPA is perceived to be lowering the standard within the Quebec legislation?” Despite the objective of Canadian privacy laws to balance privacy and innovation, inconsistent privacy laws and regulations impede both privacy and innovation. When firms either comply with the least restrictive law or gamble with noncompliance, Canadians are subject to increased misuses of their personal information. Alternatively, for firms that want to ensure compliance, they must incur increased transaction costs.

To navigate the complex set of federal, provincial and industry-specific laws and regulations, firms acquire specialized expertise and thus, face high transaction costs. Hiring a full-time privacy and compliance officer or data protection officer is an additional cost incurred to ensure privacy compliance that may not be directly related to the core product or service an organization provides. With an average annual salary of \$64,919 for privacy officers in Canada (Glassdoor 2024), the cost of retaining this expertise can be quite high. A recent survey of Canadian businesses on privacy-related issues found that only 56 per cent of businesses interviewed had a designated privacy officer, 55 per cent had a privacy policy in place and 33 per cent regularly provided employees with privacy training and education (Office of the Privacy Commissioner of Canada 2024).¹⁹ For many small and medium enterprises, they may lack the financial resources in their budget to accommodate the salary of a privacy officer, which risks increase in privacy violations. Conversely, for large organizations, such as banks, with high levels of brand awareness and consumer trust that process amounts of personal information, a privacy officer is not only a transaction cost, but also an investment.

Earning and maintaining the trust of customers is the building block of market success, while questionable activities, such as misleading advertisements, can lead to limited trust and market failure (Rudzewicz and Strychalska-Rudzewicz 2021). For a media sales director “Trust is imperative. With mobile devices people are more cautious with data” so you need to find the

¹⁹ The survey was administered to 800 companies (large to small) from November 21 to December 21, 2023, with senior decision-makers as the target respondents.

“balance between keeping trust and offering value.”²⁰ In the case of Tim Hortons’ tracking app users’ location, even when the app was not in use, the media sales director stated that “Tim’s jeopardized their trust with the customer” when the “media division wanted to leverage the geo data.” The loss of consumer trust can be a cost of noncompliance and act as a strong deterrent to these types of practices.²¹ However, for B2B firms, such as data brokers, who predominantly operate out of the public eye, the loss of consumer trust would not be a high cost of noncompliance. For data brokers violating a privacy statute could result in the political salience of their data monetization practices increasing from low to high. Consequently, this could result regulators becoming responsive to the business practices of the industry. Thus, it is in the best interest of data brokers to exploit Canada’s principle-based privacy regime and situate their business practices in the grey areas.

5.2: The Discretionary and Interpretative Landscape of Canadian Privacy Law

Compliance ensures that the collection, use and disclosure of personal information is done so with the consent and knowledge of the individual to which it belongs (First Nations Information Governance Centre 2023). However, since Canada’s patchwork landscape of privacy laws provides minimal guidance on organizational responsibilities associated with the use and storage of personal information (Milosevic and Marshall 2020), firms decide what privacy practices, policies and protections best suit their business needs. When firms are afforded this freedom and flexibility, Canadians and their personal information suffer. From designating privacy officers to justifying collection purposes to determining legitimate business interests, Canada’s quasi-self-regulatory principle-based privacy laws are easily exploited by firms to maximize profits at the expense of consumers’ privacy.

Under PIPEDA Principle 1: Accountability, Law 25 and the provincial privacy laws, there are requirements for firms to designate an individual or individuals to be accountable for the organization’s compliance with the protection of information principles. In Québec specifically, every business has an obligation, if it handles any personal information whatsoever, to have a privacy officer. The individual with the highest authority within the organization automatically assumes this role unless the responsibility is delegated to somebody else (Guilmain 2022). Despite these written requirements, there are no provisions stipulating the qualifications these designated privacy officers must possess. When firms are left to decide independently which individual is to be charged with managing the organization’s privacy practices, privacy and compliance violations increase in three ways.

First, when privacy compliance is tacked onto the portfolio of an organization’s top executive, both privacy and the business suffer. With the twin objectives of managing the business and maximizing profits, a Chief Executive Officer (CEO) may not have the bandwidth to maintain the knowledge and expertise of current regulations or the ability to disclose noncompliance knowing its impact on business objectives (Kusserow 2021). Increased privacy violations may arise if a CEO is unaware of how business is contravening a privacy statute or, is aware of the contravention but prioritizes profits over privacy. Second, for firms without a privacy officer, i.e. 44 percent of Canadian organizations, compliance can be non-existent. With no designated individual to facilitate privacy training, manage the privacy policy or provide guidance on compliance, the firm may expose itself to fines, investigations and reputational risks. The same issues may arise for firms with a

²⁰ Interview conducted with media sales director for a media buying network on April 12th, 2024.

²¹ Ibid.

designated, yet unqualified, privacy officer. Lastly, the absence of a full-time in-house privacy officer complicates complaint investigations by regulators. According to a corporate compliance, privacy and risk officer working in the Canadian insurance industry who previously investigated privacy complaints for a provincial regulator, when investigating “if you dealt with an organization that had a privacy officer that was knowledgeable the whole process was smoother. If you had a C-suite executive that was doing it off the side of their desk, it would become challenging.”²²

In terms of documenting a firm’s collection, use and disclosure of personal information in a privacy policy, the quasi-self-regulatory nature of the PIPEDA principles permits firms to establish the lowest level of compliance without being non-compliant. The PIPEDA accountability principle states that privacy policies should be “readily available to customers and employees.” However, the proportion of companies with a privacy policy has declined, from 65 per cent in 2019, to 55 per cent in 2023 (Office of the Privacy Commissioner of Canada 2024). Additionally, the likelihood of having a privacy policy is higher among big corporations than small or medium sized enterprises (SMEs). Nearly 87 per cent large business have a privacy policy compared to 67 per cent of medium-sized businesses and 53 per cent of small businesses (Office of the Privacy Commissioner of Canada 2024). The fact that 45 percent of Canadian organizations do not have a privacy policy is concerning in terms of the potential for improper uses of personal information and the powers of the OPC to enforce compliance. Another issue with privacy policies and the PIPEDA principle are firms, especially SMEs, without a designated privacy officer that rely on online tools to draft privacy policies to ‘check a box’ without any concern for customers’ privacy.

In the absence of an in-house privacy officer or legal department, firms can use an automated privacy policy generator or a large language model to create a privacy policy. For one Canadian small business owner, ChatGPT was used to draft the privacy policy for their website which was then further customized based on the types of personal information the business collects and their third-party business partners such as Canada Post.²³ To further manage and configure customer privacy settings, this small business owner also uses a customer relationship management (CRM) platform and the customizable privacy settings available through Shopify.²⁴ On the surface, these tools appear to offer firms convenient and low-cost options to provide some privacy protections. However, there are notorious issues with the quality, completeness and correctness of the policies these tools produce as they often contain unnecessary personal information collection or arbitrary commitments inconsistent with user inputs (Sun and Xue 2020).

Using the prompt “write me a privacy policy” ChatGPT created a policy that stipulates “We automatically collect certain information when you visit, use, or navigate the Site. This information does not reveal your specific identity (like your name) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Site and other technical information.” Despite no mention of these types of personal information or their use in the initial prompt, the privacy policy I generated using ChatGPT automatically included a highly invasive section on “Information Automatically Collected”. For firms seeking to monetize their customers personal information, this collection and use provisions can be easily exploited. By

²² Interview with an insurance corporate compliance and risk office conducted on April 15th, 2024.

²³ Interview with Canadian small B2C owner conducted on May 16th, 2024.

²⁴ Ibid

including all-encompassing data collection clauses in privacy policies, consumers have little control over what data firms collect, use and disclose.

Since PIPEDA and the FIPs are not prescriptive, firms are afforded a great deal of discretion in the interpretation and application of the principles. With this discretion, firms can exploit the broad and vague nature of PIPEDA to utilize personal information in ways that advance their business interests. Consequently, PIPEDA creates a quasi-self-regulatory framework that allows firms to internally justify their data collection, use, and retention purposes. Although the OPC does not utilize an enforcement pyramid or enforcement strategies pyramid, the quasi-self-regulatory and non-prescriptive nature of PIPEDA is akin to the starting point of a responsive regulatory approach. Since it would be too costly for the OPC to directly oversee the collection and uses of Canadian personal information by all firms in and/or outside of Canada, a self-regulatory approach is an attractive and useful approach, especially, in industries with rapidly evolving technologies. However, neither the market nor self-regulation are adequately protecting consumers and their personal information from data brokers. The PIPEDA FIPs, for example, afford firms too much discretion and highlight the shortcomings of a self-regulation for uses of personal information.

Principle 2 – identifying purposes – stipulates that the purposes “for which personal information is collected shall be identified by the organization at or before the time the information is collected” (Schedule 1 clause 4.2). Clause 4.2.2 expands on this provision by stating that identifying these purposes “allows organizations to determine the information they need to collect to fulfil these purposes”. The identifying purposes clause is closely tied to Principle 4 – limiting collection – whereby “both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified (clause 4.4.1). The purposes and collection of information cannot occur under PIPEDA without Principle 3 – consent. Under clause 4.3.2. knowledge and consent are required, and organizations must make a “reasonable effort” to ensure that the individual is advised of the purposes for which the information will be used or disclosed in a manner that the individual can “reasonably understand”.


In 2018 the OPC issued seven principles for obtaining meaningful consent for the collection, use and disclosure of personal information. In the context of this dissertation, the first principle, emphasize key elements, is the most relevant. This principle requires organizations to put emphasis on key elements such as for what purposes personal information is being collected, used or disclosed with sufficient precision for individuals to meaningfully understand the terms of consent (Office of the Privacy Commissioner of Canada 2018a). Additionally, this principle requires organizations to disclose with what parties’ personal information is being shared. More specifically, this subprinciple states disclosures to third parties must be clearly explained, identify the information being shared and requires firms to be as “specific as possible in enumerating these third parties” (Office of the Privacy Commissioner of Canada 2018a). On paper, the PIPEDA and meaningful consent principles create a framework where data collection and retention are not arbitrary but rooted in consent and done for a specific purpose. However, firms can exploit the flexibility of the nonprescriptive principles when establishing their purposes of collection and determining reasonability.

Since not all firms act in good faith, there are several ways these vague and broad principles can be manipulated to advance business interests. With no enforcement pyramid or enforcement strategies pyramid and limited enforcement powers, which will be discussed in the following section,

the OPC cannot gradually escalate sanctions against firms that toe the line of noncompliance without fully contravening PIPEDA. Unlike the GDPR which requires data controllers to use “clear and plain language” (Article 12), firms operating in Canada are left to interpret the meaning of reasonably understand and meaningful consent. A privacy policy riddled with technical jargon and legalese would not satisfy Principle 3 of PIPEDA. However, reasonably understands also does not mean completely understands. Firms can exploit this gap by only providing enough details on their data practices to establish a reasonable or meaningful level of understanding for customers. This creates an information asymmetry between firms and consumers as firms have a clear understanding of how they use data, while consumers have limited information on how their data is used. With insufficient information and no transparency, consumers may unknowingly consent to data collection and use clauses that they would otherwise have not accepted. Comparing the privacy policies of Canadian and French telecommunications firms highlights the weakness of PIPEDA’s vague principles.²⁵

The privacy policies of Rogers Communications and Orange S.A afford their respective customers varying degrees of details on the company’s collection, use, processing and disclosure of personal information. Rogers states that its privacy policy applies “to all personal information that we collect, use or disclose about our customers and users of our digital platform.” Specifically, this includes name, address, email, payment methods, use of products, information gathered from third parties, IP addresses, URLs, data transmission information, the time spent on websites and time on Rogers apps. Orange, conversely (see Image 2) outlines 11 types of personal information that the company processes and specifies the types of personal information that fall under each category.

Image 2: Orange Privacy Policy



Mobiles and Plans

Internet

Internet and Mobile

Remote monitoring

TV and entertainment

1. What data is processed?

Orange processes personal data concerning you as part of its relations with you and your use of its offers and services. Orange only processes data that is relevant and necessary for the objective pursued.

The personal data collected by Orange is grouped into the following categories:

Identification data	Identity (surname, first name, nickname), administrative identifier (identity card, passport, identity card or passport number, SIREN, tax identifier, Kbis, etc.), identifier issued by a non-administrative third party (Facebook account, twitter...)
Personal life	Centers of interest, marital status, household composition, lifestyle habits, customer declaring that they have an offer with a competing operator
Professional life	Job held, work organization,
Personal characteristics	Title, date and place of birth, date of death, nationality, legal protection measures, customer benefiting from social rates, physical characteristics, photo or avatar, power of attorney, signature
Contact data	Postal address, email, telephone number
Location data	Geolocation of the person or equipment associated with a person
Connection, service usage and interaction data	Connection and usage logs, traffic data, intervention report, equipment owned, technician appointment, content of a request made to Orange, disputed facts of a complaint or dispute, references of the file, start and closing date of the file, comments relating to the description and monitoring of the file, etc.
Content data	Sound, image, video, names of stored folders and tree structure
Economic and financial data	Financial identification, economic, tax and accounting data, payment history
Products and services owned or used	Offers and options owned, equipment owned, settings, content purchased, applications downloaded
Customer profile, scores and segmentation	Marketing score and segmentation, customer satisfaction indicator, good or bad payer profile and possible recovery plan, fraud risk scoring

²⁵ Conducting this comparison was suggested during an interview with a privacy specialist on May 22nd, 2024.

In terms of consent, Rogers details consent in a way that the average Canadian would reasonably understand but would not completely understand. This arises as the policy mentions implied versus expressed consent, providing one example, but does not define these types of consent or expand on how consent will be obtained for new uses of the personal information. Regarding meaningful consent, Rogers fails to identify the types of information disclosed to third parties nor does the policy enumerate the third parties to which this information is disclosed (see Image 3). Rogers also stipulates that by withholding consent there may be limits to the products and services they provide. Orange, on the other hand, lists and describes the sole purposes for processing personal information that require consent. This section also stipulates that consent can be withdrawn at any time without consequence of services not being provided and refers to the company's legitimate interest in processing information which further cites when consent is required.²⁶

Image 3: Rogers Privacy Policy



When is my personal information disclosed?

Unless we have your express consent or pursuant to a legal power, we will only disclose your personal information to organizations outside Rogers without your consent in the following limited circumstances:

- To a person who, in our reasonable judgement, is seeking the information as your agent.
- To another telephone company, when the information is required for the provision of home phone service and disclosure is made confidentially.
- To a service provider or other agent retained by us, such as a credit reporting agency, for account management, the collection of past due bills on your account, or to evaluate your creditworthiness.
- To a service provider or third party that is performing administrative functions for us to manage our customer accounts.
- To another organization for fraud prevention, detection or investigation if seeking consent from you would compromise the investigation.
- To a law enforcement agency whenever we have reasonable grounds to believe that you have knowingly supplied us with false or misleading information or are otherwise involved in unlawful activities.
- To a public authority or agent of a public authority if it appears that there is imminent danger to life or property which could be avoided or minimized by disclosure of the information.
- To a public authority or agent of a public authority, for emergency public alerting purposes, if a public authority has determined that there is an imminent or unfolding danger that threatens the life, health or security of an individual and that the danger could be avoided or minimized by disclosure of the information.
- To a third party who may be interested in buying Rogers assets and personal customer information must be shared to assess the business transaction.
- We will disclose information about your credit behaviour to credit reporting agencies or parties collecting outstanding debt.

²⁶ The Rogers Privacy Policy can be found here: <https://www.rogers.com/support/privacy/rogers-privacy-policy>
The Orange Privacy Policy can be found here: https://c.orange.fr/pages-juridiques/donnees-personnelles.html#durees_conservation

The lack of detail and clear language in the Rogers privacy policy increases information asymmetries, prevents Rogers customers from making informed decisions on how their information is being processed and punishes customers for withholding consent. As an active participant in the data-driven economy, Rogers can capitalize on its customer's personal information by exploiting the vague and nonprescriptive nature of PIPEDA. Since privacy laws in Canada take a quasi-self-regulatory approach, firms such as Rogers can meet the minimum requirements set out in the PIPEDA and provide the lowest level of privacy protections while still being compliant with the Act. By starting with self-regulation but not escalating up a pyramid of sanctions or supports depending on a firm's privacy practices, Canada's privacy regime is static, does not incentivize high levels of compliance and fails to protect personal information.

As discussed in the previous section, to address the growing privacy deficit in Canada that is arising due to PIPEDA's inability to meet the demands of the data-driven economy, the CPPA was introduced. However, similar to PIPEDA, the CPPA, as written before the dissolution of Parliament in January 2025, was positioned to afford firms a great deal of discretion in determining their purposes for data collection. The Exceptions to Requirement for Consent of the CPPA, and more specifically section 18(1)(2)(3) allows firms to prioritize their profits and interests at the expense of Canadians privacy. Section 18(1) allows organizations to "collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of a business activity" outlined in 18(2) or that a reasonable person would expect and is not used to influence an individual's behaviour or decisions. Lastly, as previously discussed, section 18(3) permits organizations to collect or use personal information without knowledge or consent if it is for an activity in which an organization has a legitimate interest.

For academics, lawyers and tech industry leaders, the harmful and privacy-undermining nature of allowing firms to decide what activities and interests require data collection cannot be overstated. Dr Brenda McPhail (2023) of McMaster University stated during her testimony on the study of Bill C-27 that section 18(3) "is a dangerously permissive exception that allows collection without knowledge or consent if the organization that wants the information decides its mere interest outweighs adverse impacts on an individual." John Lawford (2023) of the Public Interest Advocacy Center further criticized this clause in his testimony on Bill C-27 stating "the new business activities exception to consent, which is in proposed subsection 18(1), makes full use of your personal information without your consent, or even your knowledge, legal for business. Business activities are defined so widely and tautologically in proposed subsection 18(2) that only businesses will be able to define what a business is." Lastly, for Jim Balsillie (2023) of the Center for Digital Rights, testified on the study of Bill C-27 that the "legitimate business interest carve-out that allows corporations to put the pursuit of profits above the interests of consumers, where businesses are allowed to privately self-determine what constitutes legitimate surveillance and behavioural modification to trample on fundamental rights but are under no obligation to notify consumers how they are tracking and profiling them."

To avoid stifling innovation, firms operating in Canada have been afforded a great deal of discretionary power in deciding how they will protect consumers' privacy. From designating any employee as a privacy officer under Law 25 to the PIPEDA principles, to the legitimate interest exception in CPPA, firms are left to interpret these provisions in ways that best suit their business models. For data brokers, specifically, this quasi-self-regulatory framework not only fails to

prevent the sale of Canadian consumer data but encourages the mass collection of personal information. Thus, taking advantage of the vagueness of these principles' firms can expand their data processing purposes while remaining compliant with PIPEDA.

The same notion of leveraging the vagueness of the principles also applies to the sale of consumer data. Firms can either bury the consent clauses that allow for personal information to be sold in lengthy privacy policies or justify the collection of personal information as fulfilling necessary purposes. Furthermore, it is not only what is in the privacy policies that matter, but also what is excluded. In terms of selling personal information, according to Alex Cameron (2023), the co-leader of privacy and security at Fasken, privacy policies and contracts become central to the plaintiff's defence, "Don't make promises you can't keep. You don't have to say it so don't open yourself up to breach of contract." Since PIPEDA lacks prescriptive measures and affords firms a significant amount of flexibility in justifying their purposes and limits on collection, data brokers can technically comply with the Act without protecting Canadians' privacy. Thus, data brokers can easily exploit the principles-based nature of PIPEDA by interpreting the guidelines and FIPs in ways that favour their business model. All of which is done at the expense of consumers' privacy

With a non-prescriptive, quasi-self-regulatory privacy framework based on broad and vague principles business interests are pursued at the expense of Canadian consumer privacy. For data brokers, specifically, this quasi-self-regulatory framework not only fails to prevent the sale of Canadian consumer data but encourages the mass collection of personal information. Since PIPEDA lacks prescriptive measures and affords firms a significant amount of flexibility in justifying their purposes and limits on collection, data brokers can easily exploit the principles and vagueness in ways that favour and fit their business model. Additionally, under PIPEDA data brokers can have a privacy policy and be compliant without protecting privacy as they can either bury the consent clauses that allow for personal information to be sold in lengthy privacy policies or justify the collection of personal information as fulfilling necessary purposes. Even though consumer privacy and the need for firms to use data are supposed to be balanced, this section has demonstrated that across Canada's privacy regime, the pursuit of profits is prioritized over the protection of privacy.

5.3: Compliance and Enforcement: The Fate of a Powerless Regulator

Depending on what statute from Canada's patchwork privacy regime a firm violates, there are varying levels of consequences. Under CASL or the *Competition Act*, there can be severe monetary penalties and even imprisonment. Conversely, when a firm is found to be in contravention of PIPEDA, the consequences in comparison are virtually nonexistent. When the market, self-regulation and government oversight fail at preventing privacy violations, regulators should commence with persuasion to address noncompliance before moving up to punitive measures. To do so, regulators need to be responsive to the ways in which firms become non-compliant and/or exploit the grey areas between compliance and noncompliance. However, the enforcement regime under PIPEDA is reactive, weak and binary, all of which demonstrates the prioritization of profits and innovation over privacy and justice in Canada's privacy regime.

Data protection laws in Canada adopt an ombuds model to address privacy violations by both public and private sector actors. Traditionally, the ombuds model has been employed by the government to regulate public administration and monitor specialized areas of government activity. However, PIPEDA represents a novel application of the ombuds model by the

government as a means of regulating all private commercial activity, across a wide variety of industries (Stoddart 2005). With this model, a complaint must be issued prior to the privacy commissioners initiating an investigation. Under PIPEDA “an individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or 1.1 or for not following a recommendation set out in Schedule 1” (s.11(1)). Additionally, “if the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter” (s.11(2)). Within one year of receiving or initiating the complaint, the Commissioner shall prepare and deliver a report outlining their findings, recommendations, any settlements reached and the recourse available to the complainant (s.13(1)). For individuals seeking a binding order or compensation for PIPEDA breaches, they must first go through the OPC complaint process prior to applying to the Federal court. Since the Federal Court hearings are *de novo*, meaning no deference is given to the OPC’s findings, it can be “inefficient, duplicative, and does not benefit from the Commissioner’s expertise” (Scassa 2019 p. 92).

With the complaint-based nature of the OPC Ombud model, individuals must first be aware that a breach of PIPEDA has occurred. As data collection and web tracking becomes less transparent with the use of pixels and beacons, AI/ML and Big Data analytics it is becoming increasingly difficult for consumers to determine if their privacy is being violated. With large-scale data collection and sharing, the ombuds model is ill-adapted to address these complex types of privacy violations (Scassa 2019). According to a 2023 survey of Canadian business leaders conducted by PricewaterhouseCoopers (2023), 46 percent of respondents claimed to sometimes use customer data without expressed consent and 49 percent stated that they do not always vet the third parties with whom they share their customer’s data. When consumers do not know what they do not know, the usefulness of this model becomes increasingly limited. With the data broker industry, whose business practices are opaque and largely unknown, individuals cannot file complaints if they are unaware of how their data is being shared or used without their consent.

As of May 2024, there have only been three OPC investigations into the business activities of data brokers, with only one investigation arising from an individual’s complaint. In 2007, the OPC initiated a complaint against the Society for Worldwide Interbank Financial Telecommunication (SWIFT) for inappropriately disclosing records from Canadian financial institutions to the United States Treasury after receiving administrative subpoenas (Office of the Privacy Commissioner of Canada 2007). The investigation concluded that SWIFT did not contravene PIPEDA. In 2009 the Canadian Internet Policy and Public Interest Clinic (CIPPIC) alleged U.S. company Accusearch, Inc., conducting business as Abika.com (Abika), was collecting, using, and disclosing the personal information of Canadians without their knowledge or consent and doing so with inaccurate personal information (Office of the Privacy Commissioner of Canada 2009). The investigation found that Abika was in contravention of Principle 4.3. Lastly, in 2019 an individual registered a complaint against 411Numbers for using their personal information without their consent and requesting a fee along with additional information to have their original information removed (Office of the Privacy Commissioner of Canada 2019a). 411Numbers made changes to its privacy policy and ceased its practice of removing information for a fee leading the OPC to continue to monitor and review the corrective actions pursuant to the agreed-upon timeframe (Office of the Privacy Commissioner of Canada 2019a).

With these three investigations, it is important to note that they are exclusively into firms identified as ‘data brokers’, not ‘data aggregators’, ‘information brokers’ or ‘data analytics companies’. The absence of investigations into ‘data brokers’ further highlights the complexity of this industry as many of the firms on the Data Brokers in Canada List (Appendix A) do not identify as data brokers and would thus, fall outside a search of OPC investigations into data brokers. For consumers, a search of OPC ‘data broker’ investigations that only yields three results may signal that the business practices of this industry are not concerning to the OPC. However, this is not the case as a search of ‘data aggregators’, ‘information brokers’ and ‘data analytics companies’ populates 12, 36 and 4 investigations respectively.²⁷ While investigations into ‘information brokers’ are more frequent, it is the *global data broker industry*, not the *global information broker industry*, and the complaint-based model is failing to address these subtle, yet crucial nuances.

While the Canadian government may not have the time, resources nor expertise to monitor all firms that collect, use and sell data, a complaint driven model combined with self-regulation is an inadequate approach to protecting privacy. With only one individual based complaint filed against a data broker over the past 15 years, it is evident that this enforcement model fails to yield any investigations into the questionable business practices of this industry. Since data brokers utilise opaque data monetization techniques, are not consumer-facing and are often categorized ‘third party business partners’ in privacy policies, it would be extremely challenging for an individual to identify all the data brokers that possess their information let alone confirm if their data has been utilized in a manner that contravenes PIPEDA. In certain instances, with enough time, financial resources and willingness to disclose additional personal information, it is possible to determine what information certain data brokers have obtained about you. To better understand this process and any associated difficulties, I obtained my personal information from LiveRamp.

To obtain records on what personal information LiveRamp holds, you must fill out a form and verify your identity through a third party which requires a photo of a government-issued ID and an on-the-spot headshot. After completing this process LiveRamp will share an Excel document containing the personal information they have collected on you. This alphanumerically coded document provides no insights on how or where the data was obtained or specifics on the types of personal information they possess. Without this information, it is not possible to submit a complaint to the OPC against LiveRamp for collecting, using and/or sharing my personal information after completing this process as I have limited information of how my data was collected, used or disclosed to third parties and if this was done without my consent. Additionally, this complaint-based ombud’s enforcement model is further limited by Canada’s patchwork of privacy regime as individuals may be unaware of which statute applies. If an Alberta resident experiences a breach of privacy by an Alberta-based company, the Alberta Information and Privacy Commissioner under PIPA would receive the complaint (Rostama and Scassa 2023). If the complaint is against a federally regulated organization or a company in another province or outside of Canada, the complaint would be directed to the OPC with the possibility of the provincial regulator also assuming jurisdiction (Rostama and Scassa 2023). With a high barrier to entry in terms of understanding the intricacies of how personal information is collected with web tracking technologies, used in an ad tech stack or monetized by data brokers, the ombud’s model is no longer suitable for remedying privacy violations in Canada.

²⁷ OPC Investigations into Businesses can be found at: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/>

Even when the Commissioner has reasonable grounds to initiate a complaint against a firm for a privacy violation, the ombuds model and PIPEDA afford the OPC minimal powers to enforce compliance. Under section 12.1(1), when investigating, the Commissioner can summon witnesses and compel them to (a) provide written or oral testimony, (b) administer oaths, and (c) receive and accept any evidence they see fit. Additionally, section 18(1) permits the Commissioner to audit the information management practices of an organization if they surmise the organization has contravened a PIPEDA provision. The Cambridge Analytica scandal highlighted the weaknesses of the OPC enforcement powers when Facebook refused to adopt the Commissioner's recommendations and the OPC filed an application to the Federal Court for an order requiring Facebook to correct its privacy practices in compliance with PIPEDA (Karbaliotis 2020). With the Commissioner unable to issue binding orders, there are growing concerns regarding the adequacy of this model at home and abroad.

In Canada, the OPC powers are significantly reduced compared to those afforded to the provincial privacy commissioners. Pursuant to their respective PIPAs, the BC and Alberta commissioners can require that a duty imposed by the PIPA be performed and require an organization to destroy personal information collected in contravention of the Act (Gittens et al., 2018). Abroad, the OPC powers are significantly weaker than those afforded to European data protection authorities under the GDPR. With the power to levy administrative sanctions up to €20 million under the GDPR, there is concern that Canada's adequacy status with the GDPR could be revoked unless essentially equivalent powers are afforded to the OPC (Bennett 2020).²⁸ To address these weaknesses, the OPC should leverage a network of partners to increase compliance and address noncompliance. Partnering with other regulators or utilizing tripartism and working with public interest groups are core features of a responsive regulatory approach that could assist in increasing the regulation of the global data broker industry in Canada.

Despite efforts by the OPC to increase its powers under Bill C-27 and Bill C-11, the CPPA did not permit the OPC to impose administrative monetary penalties or levy fines. Instead, Bill C-27 granted the OPC power to make compliance orders and recommend monetary penalties to the Personal Information and Data Protection Tribunal. For protecting the privacy of Canadians, the Tribunal is problematic. Despite section 37(6)(4) of Bill C-27 stipulating that at least three of the members must have experience in the field of information and privacy law, section 37(6)(1) states that the Tribunal will consist "of three to six members to be appointed by the Governor in Council on the recommendation of the Minister." The fact that the Minister of Innovation, Science and Industry had such an influential role in selecting Tribunal members raises concerns for ministerial bias and conflicts of interest.

In terms of bias, the Minister often interacts with firms that collect and use personal information, not Canadians whose privacy is being commodified and violated. With lobbying, consultations and meetings with industry leaders, there is potential for the Minister to recommend Tribunal members who are sympathetic to industry interests and are thus, less likely to impose

²⁸ Article 45 of the GDPR requires that transfers of personal data to another jurisdiction can take place, without any specific authorisation, where the Commission has given that jurisdiction "adequacy status" (Coutu and Rees-Jones 2024). For Canada, this means organizations can receive personal information governed by the GDPR without additional data protections.

strong penalties for data protection violations. Additionally, with the revolving door, the Minister can recommend former C-suite executives who they previously worked alongside. The conflict of interest arising from preexisting relationships can result in the appointment of Tribunal members who prioritize the Minister's innovation agenda over personal information enforcement and regulation. Allowing the Minister to recommend Tribunal members undermines the ability of this body to make impartial decisions independent from the government. Given the Minister of Innovation, Science and Industry's mandate to "position Canada as a leader in the digital economy" (Trudeau 2021), Ministerial appointments to the Tribunal risks compromising data protection as innovation and industry will always take precedence over privacy.

In addition to the OPC's weak enforcement powers, PIPEDA and the Ombuds model also fail to consider the grey area between compliance and noncompliance that firms can easily exploit. Consequently, this further results in an enforcement framework that favours firms and innovation over Canadians and their privacy. As previously discussed, the PIPEDA principles that permit the self-justification of 'reasonably understand' and 'necessary' data collection purposes also enables firms to achieve the lowest possible level of compliance without being non-compliant. By exploiting the flexibility of the PIPEDA, firms can situate their business practices in the grey area between compliance and non-compliance, leaving no grounds for an investigation to be initiated. According to Dr Michael Geist's (2023) testimony during the study of Bill C-27, it is challenging for the OPC to ensure firms are compliant as firms will naturally engage in a bit of risk analysis asking by "What happens if I don't comply?" or "What happens if I push the envelope a little bit?" The answer is that you might face an investigation if someone realizes and files a complaint, and, at worst, at least initially, all you're going to get is a non-binding finding, and you need to try to do something." The primary challenge here is that when new or established data harvesting and/or monetization practices blur the compliance/noncompliance dichotomy, the OPC is unable to respond responsively and escalate up an enforcement pyramid.

In the marketing and advertising industry, where conversions and response rates drive profits, pushing the limits of privacy laws is a common practice. For one marketing executive, "net profit value is so key and is all tied to response rates. If you can improve that by a few points, it is so valuable. We would be willing to push for it."²⁹ When running an email campaign or pushing an advertisement using personal information, this marketing executive stated that you want a privacy and/or compliance officer who tells you "It's not that you can't do it, but here is how you can do it."³⁰ With hefty fines for noncompliance under the *Competition Act* and CASL, for this marketing executive, the value and importance of a knowledgeable compliance officer cannot be understated. Since the law is not being overtly broken, pushing the envelope is not considered noncompliance. By not taking a responsive regulatory approach to address firms pushing the envelope regulators are failing to protect Canadians from firms that manipulate grey areas to increase their profits. With the purpose of PIPEDA to balance Canadians' privacy with businesses' needs to collect, firms such as data brokers can exploit these clauses to ensure their business practices blur the lines between compliant and non-compliant.

Despite the value in partnering with a network of regulators, there are several challenges that can arise with the divergence in applicable penalties and regulatory focus. Depending on a firms'

²⁹ Interview a marketing executive conducted on May 6th 2024.

³⁰ Ibid.

misuses of personal information they may be violating several statutes that comprise Canada's patchwork privacy regime. With the rapidly changing digital economy, regulators' roles are becoming increasingly intertwined as investigations often involve a mix of competition, consumer protection and privacy concerns (Iacobucci 2021). A prominent example of the privacy/competition overlap is the parallel OPC and Competition Bureau investigations into Meta for the Cambridge Analytica scandal. The OPC concluded that Meta failed to obtain meaningful consent and adequately safeguard personal information from third parties (Office of the Privacy Commissioner of Canada 2023b). The Commissioner proceeded to file a federal court application that would require Meta to submit to ongoing supervision; however, the Court found no breach of PIPEDA. In 2023 the Federal Court of Appeals overturned this decision and held that Facebook did breach PIPEDA by failing to obtain meaningful consent from users when disclosing data to third parties and adequately safeguard user data prior to disclosure (Wall et al., 2024). Conversely, the Competition Bureau fined Meta \$9 million for making false and misleading privacy claims regarding the privacy of Canadians' personal information on Facebook. (Competition Bureau Canada 2020).

There are several issues that arise from the overlap of competition and privacy. First, the incorporation of non-economic policy issues into a competition case can render the application of the *Competition Act* unpredictable and risk arbitrariness (Office of the Privacy Commissioner of Canada 2023b). Second, in Canada specifically the Competition Bureau and the OPC have enforcement powers of varying strengths which can lead to discrepancies in terms of punitive measures for noncompliance as well as the appearance that a competition violation is more severe than a privacy violation. Lastly, there are tensions between competition and privacy. Competition policy tends to encourage the flow of data in digital environments, as a means to promote data-driven competition, while data privacy policy often leads toward added controls or limits on such data flow (Digital Citizen and Consumer Working Group 2021).

If the primary objective is to address and prevent future misuse of personal information, then the OPC should be open to the cross-over between privacy and competition regulation. To mitigate the lack of focus on privacy for joint investigations, it would be beneficial for the OPC to conduct additional investigations with the provincial privacy commissioners. By embracing the responsive regulatory view that engaging multiple actors increases the success of compliance, the OPC can better protect the privacy and personal information of Canadians. For example, in 2023 the OPC had first announced its investigation into OpenAI in April 2023 after receiving a complaint (Office of the Privacy Commissioner of Canada 2023a). However, given the broad scope and significant privacy impact of AI, the OPC along with the privacy commissioners for Québec, British Columbia and Alberta decided to jointly investigate the matter (Office of the Privacy Commissioner of Canada 2023a). While this investigation is on-going, it highlights the national and collaborative dimensions of protecting privacy.

Conclusion

For Canadians concerned with "Big Brother" government and private sector abuse of their personal information, privacy is a sense of control that enables them as individuals to set limits on both the public and the private sector (Levin and Nicholson 2005). Conversely, as seen with the patchwork of privacy laws, the quasi-self-regulatory nature of privacy statutes and the lack of enforcement power for the OPC, privacy in Canada is a barrier to innovation and economic growth.

For industries central to the data-driven economy, such as data brokers, the Canada's privacy landscape not only permits but encourages the collection, use and monetization of consumer data.

With the principle-based nature of PIPEDA, firms are afforded a great deal of discretionary power to self-justify 'reasonably understands' in terms of consent and 'necessary' purposes for data collection. For data brokers, this quasi-self-regulatory power enables them to manipulate these terms to fit their needs and make their business practices PIPEDA compliant. Since this industry is not consumer facing and operates in the shadows of the tech sector, the complaint-based Ombuds model is unlikely to result in any complaints by individuals. If the Commissioner investigated a data broker any resulting recommendations could be ignored and result in the OPC taking the firm to court, as was the case with Meta.

The reliance on self-regulation as the basis of Canada's privacy regime is failing to safeguard the personal information of Canadians, especially given the lack of enforcement powers for the OPC and new data monetization techniques that violate both the individual and group privacy of Canadians. Instead of taking a 'one-size-fits all' approach to addressing noncompliance, the OPC should employ a responsive regulatory approach that combines both punishment and persuasion to encourage compliance and reduce noncompliance. To do so, the OPC should be granted stronger enforcement powers and employ enforcement pyramids that are both industry and firm specific. Additionally, the OPC should jointly investigate data brokers with the provincial privacy regulators and engage various public interest groups, such as the Canadian Civil Liberties Association, to increase the political salience of the data broker industry.

To not stifle innovative uses of consumer data, a great deal of attention is dedicated to achieving a balance between innovation and privacy. As seen with the purpose of PIPEDA, it is evident that for the Government of Canada it is possible to balance a firm's need to use data and an individual's desire to protect their personal information. However, for Dr Michael Geist (2023), "...the playing field will never be balanced. It's always tilted in favour of businesses." As will be discussed in the next chapter, the alignment of corporate and government interests around profits and economic growth results in a framework that places business interests ahead of privacy. Even with Bill C-27, the inclusion of the legitimate interest clause and the removal of consent requirements promotes the collection and monetization of data further tips the scales in favour of corporate interests, profits and growth. For data brokers, the features of Canada's privacy framework discussed in this chapter not only fail to regulate their business practices but encourage their data monetization practices. As PIPEDA becomes increasingly outdated vis-à-vis new data harvesting methods, Canadians will have increasingly less powerful protections in place to safeguard and govern how their data is used and monetized by firms such as data brokers.

Chapter 6: The Interests and Influence of the Global Data Broker Industry

Introduction

For Miriam Smith (2017), the market system reinforces business power without any action on the part of the business community. While this may be true, it does not negate the fact that independently and collectively, firms allocate a great deal of time, effort and money to influence governments and advance their private interests. As a means to the end of improving regulatory environments and increasing profitability, firms can exercise their business power to weaken a regulation, redirect a policy, or prevent a specific bill from being passed. Depending on the extent of the influence laws, policies and regulations may be consistently or repeatedly directed away from the public interest and toward the interests of private firms. For example, regulatory capture has been characterized as the greatest obstacle to Canada meeting its greenhouse gas emission reduction targets (MacLean 2019). In this case, a diagnosis of a strong degree of regulatory capture can be given. However, the impact of private influence is not uniform across all industries and regulatory bodies.

Since regulatory capture must be measured in degrees, this dissertation empirically distinguishes between capture and business power but views Fuch's three dimensions of business power as operating alongside regulatory capture. In doing so, this dissertation and chapter treat regulatory capture as an important question regarding business power. For example, through lobbying, (instrumental power) firms can advance their interests and shape, weaken or redirect laws, policies and regulations. The lobbying activities of firms can be formal, as will be discussed in this chapter, or informal (i.e. through invitations to sporting events, company parties or social outings). Despite these negative connotations, lobbying is not inherently negative or problematic. According to a former lobbyist, "The government cannot exist in a vacuum, they need to hear from industry. It is part of the government process. It creates a healthy feedback loop."³¹ Lobbying, however, is not the only avenue through which organizations advance their business interests.

This dissertation and chapter also highlight the ways in which industry can thrive without a strong degree of capture and the more subtle forms of power that come from the structural position of business within the economy as well as the alignment of government and commercial interests. Using discursive and structural forms of power, organizations can create jobs, provide expertise to government officials, run advertising campaigns to shape public opinion or offer future employment opportunities legislators and regulators. Through these avenues of influence independently or in tandem, firms and business associations can work to ensure their industries remain favourably regulated. This is not to say all business power results in a strong degree of regulatory capture. Instead, the absence of industry specific regulations may be unrelated to capture and instead is attributed to a set of secondary contributing factors. With the global data broker industry's operation in Canada, this chapter investigates the ways in which this industry and the firms that comprise it exercise their business power to determine if the absence of a specific data broker regulation is attributed to their private influence or a combination of other factors.

Utilizing capture theory and the literature on business power, this chapter presents and examines two primary and three secondary avenues of influence through which data brokers can

³¹ Interview with a former lobbyist conducted on June 30th, 2024.

but are largely not exercising their three forms of business power to redirect or weaken privacy regulation. The two primary avenues of influence are the alignment of corporate and government interests (structural and discursive power) and lobbying (instrumental power). The three secondary avenues of influence are committee hearing testimony, industry associations and government partnerships, all three of which operate across the three forms of business power (instrumental, structural and discursive form of power).

Through the analysis of these five channels of business power, this chapter contends that the overall lack of regulation of the data broker industry in Canada is not due to a strong degree of regulatory capture arising from data brokers effectively exercising their three forms of business power. Instead, there is a very weak degree of regulatory capture as the absence of regulation can be attributed to the Government of Canada's reliance on a self-regulating tech sector to avoid stifling innovation, alignment with business interests in terms of maximizing profits, and minimal knowledge on the data broker industry. Together, these three factors create a favorable regulatory environment that data brokers need not disrupt by exercising their private interest influence to weaken or re-direct policies and thus, calling attention to their industry.

Chapter 6 is organized as follows. Section 6.1 presents and examines a set of economic assumptions employed by data brokers to enable the monetization of personal information policymakers to encourage data driven business practices that fuel Canada's digital economy. Section 6.2 focuses on the presence and absence of formal lobbying activities of traditional and digital age data brokers in both the U.S. and Canada. Lastly, Section 6.3 examines three additional avenues of influence through which data brokers can but largely refrain from exercising their three forms of power to advance their business interests.

6.1: Justifying Data Monetization with Economics Assumptions

Marked by automation, computerization and the shift of investment from tangibles to intangibles, the fourth or digital industrial revolution continues to impact and reshape the Canadian economy (Faucher and Houle 2023). The contribution of the digital economy to Canada's gross domestic product (GDP) increased from \$104 billion in 2017 to \$123 billion in 2020 (Statistics Canada 2023). Given the centrality of data to the digital economy, the growth of Canada's digital economy can be attributed to the profits generated from the monetization and commodification of personal information. To promote this growth, the Government of Canada relies on a self-regulating tech sector and non-prescriptive privacy regulations. By doing so, there is an alignment of corporate and government interests rooted in their mutual interest of maximizing revenues and reaping the benefits of free-market capitalism. For data brokers, this shared ideological ground minimizes the need for these firms to exercise their discursive and structural power as this power is afforded to them through a predetermined set of economic assumptions underpinning the capitalist system that justifies their business practices. This section presents and examines these economic assumptions to illustrate how their use has contributed to the growth of the data broker industry in Canada and the pursuit of profits over privacy.

The data broker industry and information markets are built on the premise that disclosing data is an economic market-based decision made by rational utility-maximizing consumers. Even as the Government of Canada seeks to modernize its private sector privacy regime, the notions of consumer rationality, intervention stifling innovation, and firms' rights to use data persist. Most notably, the title of PIPEDA's replacement, the *Consumer Privacy Protection Act*, highlights the

view that in the eyes of the government, Canadians are not individuals but are in fact, consumers. Across the U.S., residents of Indiana, Iowa, Kentucky, Minnesota, Montana, Oregon, Utah and Virginia are also seen first and foremost as consumers under the *Consumer Data Protection Acts* of their respective states. In California, within one year of the *California Consumer Protection Act* coming into force, the Act was amended and the title changed to the *California Privacy Rights Act*. Despite removal of consumer from the title, the Act still refers to and defines California residents as consumers. By viewing individuals as consumers and personal information as data, firms and governments can focus on increasing revenues and stimulating economic growth with minimal concerns for individual well-being or sustainability.

The assumption of rationality is a core principle central to liberal market economies and capitalist economic systems. Basic notions of economic rationality provide a means of determining whether individuals' privacy choices are based on maximizing their utility or well-being (Lee and Weber 2024). Thus, when presented with the opportunity to share data in exchange for free services or discounts, it is assumed the rational consumer would be willing to make this exchange as it is aligned with their self-interest. For the Digital Advertising Alliance of Canada (DAAC) (2024), "with interest-based advertising, you get ads that are more interesting, relevant, and useful to you. Those relevant ads improve the online experience and help users find the things that interest them more easily. There is another benefit for you as well: free or lower-cost products and services." For advertising industry association such as the Interactive Advertising Bureau (IAB) Canada, interest-based advertisements are not only beneficial to consumers in terms of receiving free online content, "the ads function as a valued service rather than an interruption to their browsing experience" (Office of the Privacy Commissioner of Canada 2011). By highlighting the economic benefits and concealing the costs of disclosing data, data brokers and related industry associations can play to pre-existing economic assumptions about consumer rationality and thus, generate more fuel for the data-driven economy.

The reliance on market-based approaches to privacy including notice and consent strategies coupled with advances in AdTech, data mining and Big Data analytics further obscures the costs and negative externalities (such as data being shared with third parties) of disclosing data. Even if individuals had access to complete information, they would be unable to process and act optimally on vast amounts of data as privacy intrusions are complex, multifaceted and context-specific (Acquisti and Grossklags 2005). When consumers make rational decisions based on their perceived benefits, but not costs, they may be willing to exchange their personal information for various goods and services. However, with information asymmetries between firms and consumers, the notion of a rational utility-maximizing consumer vanishes as neither a rational nor utility-maximizing decision can be made when firms promote the benefits and conceal the costs of using their products and/or services.

For example, Intuit (2024), the parent company of Credit Karma, QuickBooks, TurboTax and MailChimp, uses phrases such as "Your data works for you" and "How we put your data to good use" on its Privacy and Security webpage to convince customers that disclosing their personal and financial information is in their best interest. Through its communicative practices, Intuit is also utilizing and building on the long-standing notion that consumers are self-interested and desire to maximize their utility to advance their business interests. To further encourage and entice the disclosure of information, Intuit highlights the benefits of information sharing through statements

such as “Our offerings show you up-to-date recommendations and insights based on your data so you can make the financial decisions that are right for you” and “Not only can we suggest which loans or credit cards might be a good fit for you based on your specific situation, but we can also help you apply for them with the click of a button” (Intuit 2024b). What Intuit does not highlight on this webpage, but instead buries in its privacy policy is its use of web beacons and pixels for tracking, sharing of personal information with advertising networks, and partnerships with data providers i.e. data brokers (Intuit 2024a). All of which produces additional streams of revenue for Intuit and can result in consumers incurring the costs, as discussed in Chapter 3, of this decision at an unknown later date.

Both off and online, consumers continually engage in privacy-seeking behaviours to protect their personal information (Acquisti, Brandimarte, and Loewenstein 2020). In information markets where personal information is exchanged for goods or services, there is no opportunity to protect one’s privacy as the options are binary. For example, upon downloading TikTok users are presented with a popup banner that says, “By tapping ‘Agree and continue’, you agree to our Terms of Service and acknowledge that you have read our Privacy Policy to learn how we collect, use and share your data.” From here, users have the option to click on and read the Terms of Service and/or Privacy Policy, however, regardless of their engagement with these documents users cannot “Deny and continue”, select the types of data they consent to provide or decide which data they do not permit to be collected. Instead, users can either tap “Accept and continue” to proceed to the app or decline the terms forgo access to the app entirely. This ‘all or nothing’ approach affords firms such as ByteDance, the parent company of TikTok, with unchecked power to determine how and under what conditions users will interact with their app.

The control afforded to firms to make these types of decisions stems from two assumptions. First, privacy protections are redistributive and create market inefficiency (Lee and Weber 2024) and second, state intervention in the tech sector would stifle innovation, creativity and in turn, the market (Regan 2003). The desire to leave firms to control markets and enhance their own profitability has been an inherent feature of capitalism since the days of Adam Smith (Cutler et al., 1999). With the copious amounts of wealth generated from the rise of automated computer systems in the 1970s and the e-commerce boom in the late 1990s, technology and Internet pioneers in the U.S. were left to pursue their business models unencumbered by government regulation (Smyth 2019). Largely attributed to the landmark *Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995)*, in which Prodigy was found to be a publisher, rather than a distributor due to its selective content moderation practices, and thus liable for defamatory posts made on its bulletin boards, legislators enacted Section 230 of the U.S. Communications Decency Act of 1996 (47 U.S.C. § 230) to ensure the Internet would continue to flourish. Section 230 grants platforms broad ‘safe harbor’ protections against legal liability for any content posted on their platforms by third-parties (subsection (c)(1)) and, affords platforms discretion in moderating and removing posted content without incurring liability (subsection (c)(2)) (Smith and Alstyne 2021). By preventing online platforms from being treated as publishers, no statute has been more instrumental in the rise of Big Tech or the growth of the Internet than Section 230 (Rozenstein 2024).

With no liability for user-generated content and the discretionary power to set rules around content moderation, Section 230 has and continues to enable platforms to host a broad spectrum of content thereby attracting a large and diverse userbase whose data can be collected and

monetized through advertising.³² Despite longstanding notions of a right to be let alone in American legal literature, as discussed in Chapter 2, the combination of Section 230 and the lack of regulatory oversight for the tech sector, especially in terms of privacy, created the ideal conditions for search engines and social networking sites such as Google and Facebook to leverage vast amounts of user data to grow their advertising-driven revenue models.

To avoid stifling innovation and thus reducing profits, firms and industry associations across the tech sector have been left to self-regulate. With this self-regulation, the tech firms of the 1990s and 2000s set the rules for data driven business models, created markets for personal information and determined what types of personal information can be monetized with little to no state interventions. For individuals, a consequence of this self-regulation and rule-setting power is the sharing of data knowingly or unknowingly with third parties. A notable example is the Cambridge Analytica scandal which involved the illegal harvesting of personal data from 50 million Facebook users to build detailed profiles on U.S. voters in order to target them with personalized political advertisements in the 2016 Presidential election (Cadwalladr and Graham-Harrison 2018). Even as privacy statutes are enacted or updated, and online service providers offer users more privacy protections, the assumption that self-regulation promotes innovation persists and thus, continues to dictate how firms collect, use, store and monetize personal information.

With the emergence of data-driven business models and information markets alongside the commodification of data, consumers, or more accurately the producers of this commodity, have been excluded from data transactions and have lost control over their information. The speed at which firms collect, analyze, and distribute consumer data is enhancing their profitability while simultaneously exacerbating privacy concerns (Elvy 2018). The erosion of individual privacy brought about by technological change, institutional forces and an increasingly outdated privacy regime has resulted in individuals losing control over their personal information (K. Laudon 1996). The loss of control arises when the data is collected, shared, hacked or breached. In terms of data collection and sharing, since the data is tracked and stored in the information systems built and managed by firms, it is assumed the property rights over the data are held by the firms, not the individuals themselves (Li et al., 2023; Varian 1997). By possessing and controlling the flow of personal information, firms can monetize this asset through any of the business practices discussed in Chapter 4 with minimal interference from consumers and/or regulators. With this ownership and control, firms have an endless supply of data to fuel the data-driven economy. For governments, the data-driven economy presents lucrative opportunities to increase tax revenues and GDP. Thus, by supporting and encouraging the notion that personal information is the property of firms, states are reaping the economic benefits of consumer data commodification

In addition to firms having property rights over the data in their systems, many privacy statutes provide firms with a legal basis for collecting a processing data. In Canada, PIPEDA governs yet permits the collection, use and disclosure of personal information and the Legitimate Interest clause (18(3)) in Bill C-27 would have allowed and encouraged firms to collect and use personal information. Canadian regulators also subscribe to the view that firms, rather than individuals, own and control personal information. As stated by Canada's former Privacy

³² Given this dissertation's focus on the intersection of data monetization, privacy and regulation, the use of platforms to incite violence and hatred, spread misinformation and exploit children as well as the subsequent lack of culpability for Big Tech in the perpetration of these harms are important areas of research but will not be discussed.

Commissioner, Daniel Therrien (2023) during his testimony on Bill C-27 “there is still value in people controlling their information to the greatest extent possible, but realistically, we know that we're no longer in that world. It is simply not realistic to think that citizens can provide consent in each and every case when information is used”. As seen in Chapter 5, for individuals, Canada’s quasi-self-regulatory and non-prescriptive privacy regime is exacerbating their loss of control and ownership over their data as firms can self-justify their data collection purposes. Moreover, the weak, static and reactive OPC is failing to adequately safeguard personal information, prevent noncompliance and encourage compliance all of which signals the need for a modernized enforcement model that is responsive, flexible and adaptive.

With the state highly dependent on firms for tax revenues in a capitalist system, the alignment of corporate and government interests in favourable regulations, opening new markets and fostering innovation creates a strong predisposition for firms interests to be prioritized. For data brokers, the economic assumptions discussed above provide the underlying framework that has allowed the industry to not only survive but thrive. The assumption that individuals are consumers who make rational decisions to maximize their utility, such as exchanging their data for free goods and services, promotions and/or discounts has given the data broker industry an endless supply of data. Since the state already views individuals as rational consumers, there is minimal need for data brokers to exercise their structural or discursive power to shape narratives on consumer behaviour, the economic benefits of their industry or the value in monetize data.

For the digital age data brokers such as rewards programs and credit cards, market research companies and Big Tech platforms, incentivizing rational consumers to disclose their data is easily done by focusing on the perceived benefits they provide. Once obtained, this data can be sold to traditional data brokers or used to serve targeted advertisement campaigns as the firm, not the individual has property rights over the data. Based on the assumption that firms have the right to use their resources to generate profits, firms have been granted ownership over the data they collected and are thus, legally allowed to sell the data. With self-regulation, tech firms have previously established the rules of the game and have created markets to buy and sell personal information without government intervention. Thus, today there is minimal need for data brokers specifically to exercise their structural power to reshape rules and create markets that already favour their business interests. In terms of diagnosing capture, the alignment of government and corporate interests and the subsequent absence of data brokers exercising their discursive and structural power is one of three prongs that points to a very weak degree of regulatory capture.

6.2: Don’t Poke the Bear: Data Broker Lobbying in Canada and the United States

With significant financial resources at their disposal, firms and business associations shape regulatory landscapes, influence policy making and advance their interests through lobbying. In the 2023-2024 fiscal year, over 34,200 communication reports were filed in Canada’s Registry of Lobbyists, detailing the written or spoken communications between lobbyists and designated public office holders (DPOH) regarding regulated matters (Office of the Commissioner of Lobbying of Canada 2024). By lobbying firms and business associations can shift the focus of these regulated matters away from the public’s interest and towards their private interests. When laws, regulations and policies are repeatedly redirected in such a manner a diagnosis of regulatory capture can be given. However, as discussed in Chapter 3, regulatory capture is not binary thus, any diagnosis of capture must also determine the degree of the regulatory capture.

Focusing primarily on instrumental power, this section assesses the lobbying activities of data brokers in the U.S. and Canada, illustrates that the under-regulated data broker industry in Canada cannot be attributed to formal registered lobbying and provides further support for the very weak diagnosis regulatory capture. Additionally, this section posits that since the data broker industry receives minimal attention from legislators and regulators, it is in the best interest of these firms to avoid lobbying and calling attention to their business practices and the weak regulatory environment that favours these practices.

Despite the growing number of privacy laws and policies that are being updated or implemented and around \$178 billion in global revenues (Twetman and Bergmanis-Korats 2020), there is minimal formal lobbying activity being undertaken by data brokers in the U.S. and Canada. As discussed in Chapter 3, to evaluate the lobbying activities and influence of data broker in Canada and the U.S, I elected to focus on the federal level. Since California is the most populous U.S. state and home to Silicon Valley, I utilized the firms listed on California’s data broker registry to complete the proceeding analysis. Using this registry and the digital age data brokers identified in Chapter 4 that fall outside this list, there are 562 data brokers operating in the U.S., 27 of which have formally lobbied the federal government. In Canada, of the 150 data brokers identified on the Data Brokers in Canada List (see Appendix A), 20 firms have actively lobbied the Government of Canada with only 11 lobbying on issues related to privacy and access to information. The difference in industry size between the U.S. and Canada can be attributed to the significantly larger American economy and population. In 2023, the U.S. population and GDP were 334 million and \$27.72 trillion (USD) respectively while Canada’s population and GDP were 40 million and \$2.7 trillion respectively (USD) (World Bank Group 2024a, 2024b). To account for the differences in market size between Canada and the U.S., I will use percentages when analysing the lobbying activities of data brokers.

In Canada, only seven percent of the identified data brokers have registered to lobby the Canadian government on issues pertaining to the subject matter category of privacy and access to information (see Table 4). Of the data brokers that comprise this 7 percent, 73 percent are classified as digital age data brokers and 27 percent are traditional data brokers. More specifically, 55 percent of the digital age data brokers are Big Tech firms and 18 percent are AdTech firms. In total, only 5 percent of digital age data brokers are registered as lobbying the Government of Canada. In terms of the traditional data brokers, there was one

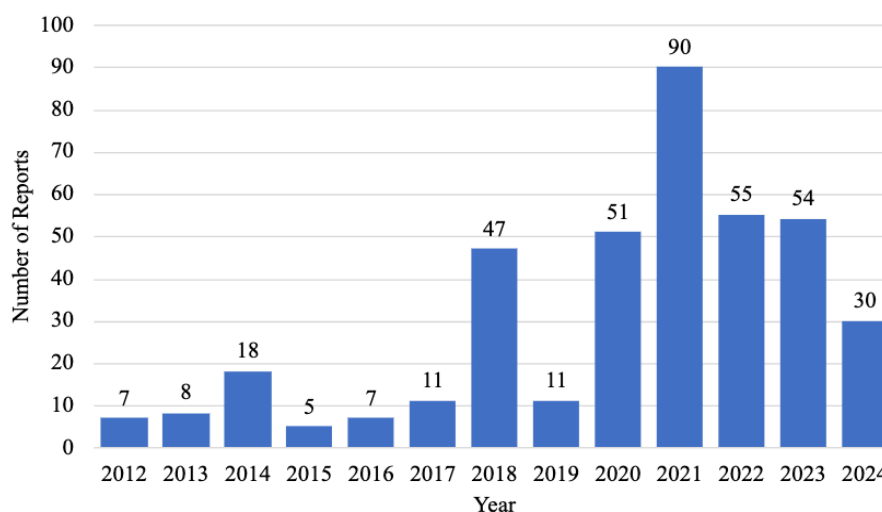
Table 4: Communication Reports Filed by Data Broker

Data Broker	Communication Reports Filed	Years Reports Were Filed
Amazon	125	2018 – 2023
Equifax	5	2016
Facebook	14	2014, 2021, 2024
Google	48	2012 – 2014, 2016 – 2018, 2020, 2022, 2023
IQVIA	37	2022 – 2024
Microsoft	39	2015, 2017, 2021, 2022, 2023
Salesforce	7	2012, 2022, 2024
SAP	1	2020
TikTok	95	2020 – 2024
TransUnion	15	2017, 2018, 2020, 2021

personal health information data broker (IQVIA) and two financial information data brokers (Equifax and TransUnion) lobbying the Canadian government. In total, only 2 percent of traditional data brokers have engaged in registered domestic lobbying activities in Canada. With only 7 percent of data brokers in Canada lobbying to advance their private interest, there is minimal evidence of these firms exercising their instrumental power through formal registered lobbying to advance their interests.

In addition to the limited number of data brokers that have formally lobbied the Canadian government, the number of monthly communication reports filed by or on behalf of these firms also points to an absence of instrumental power being exercised by data brokers. Between January 2012 and September

Chart 1: Communication Reports Submitted by Data Brokers



2024, lobbyists working for or with these 11 data brokers filed a total of 393 communication reports (see Chart 1). The near 400 communications between data broker lobbyists and DPOH on privacy related issues would be an initial indicator of these firms exercising their instrumental power to advance their interest. During this period DPOHs in the House of Commons and Innovation Science and Economic Development Canada (ISED) were the top two government institutions lobbied with 177 and 74 communication reports respectively. In this same timeframe only three communication reports were filed for DPOHs at the Office of the Privacy Commissioner of Canada and 16 were filed for DPOHs in Justice Canada.

Since MPs and DPOHs in ISED play a pivotal role in tabling, studying, supporting and overseeing the privacy statutes discussed in Chapter 5, the fact that these two institutions received the most privacy related communications could also point to these firms actively exercising their instrumental power, working to redirect or weaken privacy related laws and thus, a strong degree of capture. However, considering the 12-year span in which the 393 communications reports were filed, it becomes evident that there is not sufficient evidence to diagnose a strong degree of capture based on the formal registered lobbying activities of data brokers. Instead, the minimal formal registered lobbying activities of data brokers is utilized in combination with the absence of structural and discursive power presented in section 6.1 as well as the forthcoming discussion on the secondary avenues of influence not being utilized by data brokers in section 6.3 to diagnose a very weak degree of regulatory capture. With an average of 30 communication reports filed between 2012 and 2024, peaking with 90 reports in 2021 (see Chart 1), the absence of data brokers

exercising their instrumental power to advance their interests is further supported despite the increasing number of reports filed annually.

Similarly to Canada, there is minimal evidence of data brokers formally lobbying the U.S. federal government to advance their private interest. In 2023 and 2024, only 5 percent of the identified data brokers lobbied the U.S. federal government. Table 5 identifies these data brokers, many of which are included on The Data Brokers in Canada List included in Appendix A. More specifically, their data and privacy related lobbying fell under one of 17 general issue areas including advertising, consumer issues, safety and protection, computer industry, health issues, financial institutions, investments and securities, telecommunications and trade.

Of the data brokers that lobbied in 2023, 70 percent of their lobbying on data and privacy fell under the issue area of consumer issues, safety and protection (see Chart 2). Additionally, 63 percent of the firms filed lobbying reports

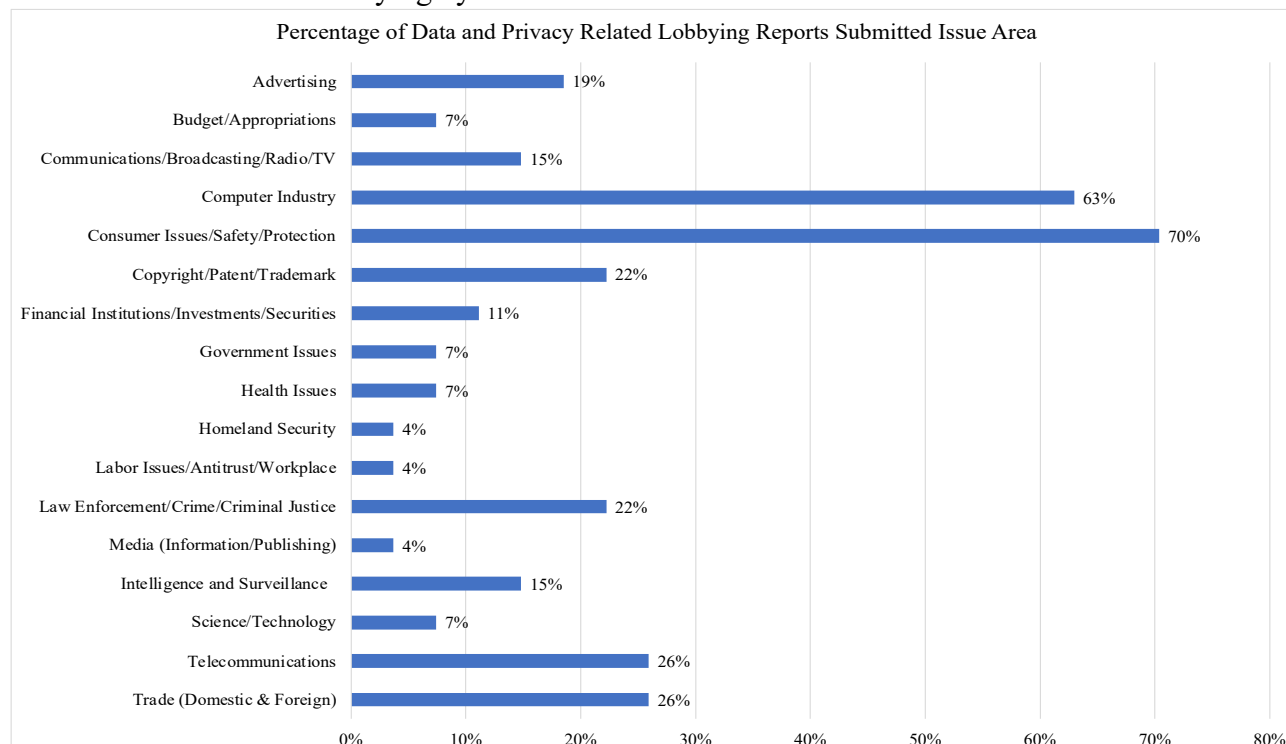
related to data and privacy under the computer industry issue area and 26 percent filed reports under both trade and telecommunications. Under these general issue areas, the data brokers and their in-house or hired lobbyists sought to target various regulations, policies and legislations, provide strategic counsel specific matters and/or lobby on specific issues. For example, under computer industry and intelligence and surveillance Meta spent \$30,000 to lobby the U.S. Senate on “Issues and discussions related to technology and the Internet including privacy, data security, research, online advertising, Section 230 and online issues of discrimination, targeted harassment and cyberstalking. Discussions regarding content transparency efforts and issues related to the S.486 Honest Ads Act” (Blue Mountain Strategies 2024). Under the category of trade Salesforce lobbied on “information technology issues, global data flows, international trade agreements and

Table 5: U.S. Data Brokers that Lobby

Data Broker	Type of Data Broker
Acxiom	Traditional: Marketing and Advertising
Amazon	Digital Age: AdTech, Big Tech
Aristotle International	Traditional: Marketing and Advertising
Equifax	Traditional: Financial Information
Experian	Traditional: Financial Information
Google	Digital Age: AdTech, Big Tech
Gravy Analytics	Traditional: Marketing and Advertising
IQVIA	Traditional: Health Information
LinkedIn	Digital Age: Big Tech
LiveRamp	Traditional: Marketing and Advertising
MediaOne	Digital Age: AdTech
Meta	Digital Age: AdTech
Microsoft	Digital Age: Big Tech, Marketplace
Oracle	Traditional: Marketing and Advertising
Pinterest	Digital Age: Big Tech
RELX Group (LexisNexis)	Traditional: Marketing and Advertising, Financial Information
Roku	Digital Age: AdTech
Salesforce	AdTech, Marketplace
Snapchat	Digital Age: Big Tech
Spotify	Digital Age: Big Tech
T-Mobile	Telecommunications
TikTok	Digital Age: Big Tech
TransUnion	Traditional: Financial Information
Twilio	Traditional: Marketing and Advertising
X Corp	Digital Age: Big Tech
ZoomInfo	Traditional: B2B

international privacy agreements” (Franklin Square Group, LLC 2023), while Snapchat lobbied to “provide strategic counsel on matters related to data security and other issues affecting the company” (BGR Government Affairs 2023).

Chart 2: Data Broker Lobbying by Issue Area



With less than five percent of the identified data brokers formally registered as lobbying the U.S. government, the degree of regulatory capture in the U.S. is also very weak. However, in contrast to Canada, there was a higher percentage of traditional data brokers that lobbied the U.S. federal government in 2023 - 2024 (see Table 2). Of the five percent of data brokers that engaged in lobbying activity, 52 percent were digital age data brokers and 41 percent were traditional data brokers. More specifically, for the digital age data brokers 44 percent were Big Tech firms and seven percent were AdTech. For the traditional data brokers, 4 percent were B2B brokers, 11 percent were financial information brokers and 22 percent were marketing and advertising data brokers. As is the case in Canada, there is a higher percentage of digital age data brokers lobbying the American government opposed to the traditional data brokers. In both Canada and the U.S. only two percent of the identified traditional data brokers are formally lobbying. Regarding the digital age data brokers, there is a higher percentage of these firms lobbying in Canada than the U.S. with five and three percent respectively. Despite this marginal difference, in both Canada and the U.S., data brokers are largely not exercising their instrumental power through formal registered lobbying to advance their business interests.

Even with a limited amount of formal registered lobbying, the lobbying activities of these firms, especially the digital age data brokers, is not zero. The higher percentage of digital age data brokers lobbying in both Canada and the U.S. opposed to the traditional data brokers can be attributed to the overall lobbying activities of Big Tech firms. Since Big Tech platforms lobby on

various subject matters beyond privacy³³, face numerous other forms of regulatory scrutiny and are used extensively by the public, lobbying does not risk exposing their industry or business practices. For example, the frequent appearances of CEOs from Big Tech platforms such as Amazon, Google, Facebook and X before U.S Congressional committees to address privacy, anti-trust and election interference concerns highlights both public and government awareness of these firms' business practices. Conversely, for traditional and the other digital age data brokers, lobbying would draw attention to their profitable business practices that are largely unknown to federal legislators and regulators.

The lack of formal lobbying by data brokers in Canada and the U.S. can be attributed to two interrelated factors. First, by lobbying to advance their interests, data brokers would be calling attention to their profitable business practices that are largely unknown to federal legislators and/or regulators. As discussed in Section 6.1, the notion that regulation stifles innovation enabled the data broker industry to grow in the shadows of the tech sector by monetizing various types of personal information without government oversight. With no industry specific regulations, data brokers run the risk of 'poking the bear' and exposing their business practices and industry size by lobbying. Moreover, with Canada's quasi-self-regulatory privacy framework which does not include any enforcement pyramids, data brokers need not lobby to maintain their position at the base of the pyramid or minimize any escalation in sanctions for noncompliance.

Since data brokers are B2B firms and operate largely out of the public eye, engaging in quiet politics is advantageous as it keeps their uses of personal information an issue of low political salience. The data harvesting and monetization practices of these firms are invasive, widespread and all encompassing. If the public became aware of the lucrative and privacy violating business practices of data brokers, it would become increasingly difficult for Canadian and American policymakers to not impose industry specific regulations. Given the lack of attention given to the data broker industry by Canadian federal regulators and legislators as well as a privacy regime that prioritize profits over privacy the need for data brokers to lobby is minimal.

The formal registered lobbying activities of data brokers presented and discussed in this section were utilized to evaluate the degree to which this industry employs its instrumental power to shape, weaken or redirect privacy laws and regulations to advance their private interests. Through this analysis, it was concluded that the formal registered lobbying of data brokers, in both Canada and the U.S. is rather limited. For the Canadian case, this finding is the second prong utilized to diagnose a very weak degree of regulatory capture by the data broker industry.

6.2.1: Limitations with Lobbying Data

To evaluate the lobbying efforts of data brokers in Canada and the U.S., I utilized the lobbying databases published by the Office of the Commissioner of Lobbying of Canada and OpenSecrets, a Washington, DC based non-profit that tracks data on campaign financing and lobbying. These datasets and disclosures of formal lobbying provide valuable insights into the influence-seeking activities of various firms, however, there are several limitations on the insights that can be generated using this data.

³³ For additional information on the lobbying activities of Big Tech platforms in Canada visit [The Tech Lobby Project](#) led by Sara Bannerman of McMaster University.

In Canada the lobbying registration dataset can be utilized to produce a list of firms that have lobbied on specific policies, programs, bills, or regulation as well as more broad subject matter categories such as privacy and access to information. However, since a lobbying registration can contain multiple subject matters, bills or regulations and government institutions lobbied, it is not possible to determine which institution was lobbied for a specific issue. Additionally, since a registration can be updated to include new subject matters, without a new registration being filed, it is also not possible to ascertain when a specific institution was lobbied on a certain issue. With these limitations it cannot be determined when IQVIA or TikTok formally lobbied ISED on privacy related issues.

To obtain additional information on the formal lobbying activities of firms, the monthly communication reports data set must be used. With this dataset one can determine when a specific DPOH was lobbied and by what firm. However, this dataset only details the broad subject matter of the communications, not the regulations, legislations and/or policies discussed in these communications. To determine when a specific DPOH was lobbied on a specific policy, legislation or regulation, the dates on when the registration was filed and when the communication took place can be cross-referenced. Unfortunately, due to the reporting requirements for lobbyists and the data contained in each dataset, there are minimal instances when a lobbying registration can be tied to a specific communication report.

An additional limitation of using lobbying data is the great deal of informal lobbying that fall beyond the scope of activities capture by the registry. This can include innovations to sporting events, company events or dinners. According to one lobbyist the federal lobbying registry also does not capture the grey area of lawyers that advise and see themselves as lobbyists but do not formally register as lobbyists. This is not to say that all lobbyists work outside the system or do not report their communications with DPOHs. In fact, it is quite the opposite as for a former lobbyist, “lobbyists get a bad reputation, there are creeps, but you get those in every industry.”³⁴

Similarly to the challenges with using the lobbying registration data for Canada, the lobbying reports for the U.S. also provide a limited number of insights. Beyond determining which firms have lobbied on a general issue area (such as trade or computer industry) the lobbying reports provide some additional details on the specific lobbying issues. These details, however, are limited to ‘issues on privacy’ or ‘issues related to consumer protection and data privacy’. The available data also only provides insights on the government agency lobbied, but not the specific government official that was lobbied. For many of the lobbying registrations, the target of the lobbying activity is the U.S. House and Senate. While the U.S. lobbying registrations provides details on the lobbying expenditures of the firms, the registrations contain multiple issue areas are updated quarterly and include various government agencies. Consequently, other than in rare instances, it is not possible to determine how much money was spent by a specific firm on a specific issue.

Despite the limitations of the federal lobbying data available in Canada and the U.S., there was sufficient data to determine that in both countries data broker lobbying is rather limited and that there is a very weak degree of regulatory capture. This diagnosis of capture is further explained by the fact that there is no benefit or need for data brokers to lobby in Canada as the industry

³⁴ Interview conducted with a former lobbyist on June 30th, 2024.

benefits from Canada's current and proposed privacy statutes and not calling attention to their lucrative data monetization business practices.

6.3: Additional Avenues of Influence

In addition to pushing certain narratives, shaping the rules of the game and lobbying, firms can shape, redirect, or undermine political processes through various avenues. Using the three forms of business power firms can encourage personal donations from executives and/or employees to a specific candidate (instrumental), launch public awareness campaigns to shape opinions (discursive) or threaten to relocate jobs and investments (structural). The effectiveness of these avenues of influence depends on the firms' size, financial resources, the political salience of a specific issue and level of formality of the governing institution. For example, when firms attempt to influence tax policy "they have to work through political parties or by persuading public opinion. The tools of quiet politics do not work in the arenas of institutional choice dictated by high salience and formal institutions" (Culpepper 2010, p. 186).

As discussed in the previous section, data brokers benefit from their data collection and monetization practices being an issue of low political salience. To maintain this status-quo it is in the best interest of the data broker industry to engage in quiet politics. This section presents three additional avenues of influence through which data brokers can exercise their business power in Canada. However, since Canada's privacy regime favors their business practices and exercising their power would call unwanted attention to their industry, data brokers have a minimal need to utilize their business power to shape and/or influence legislative processes or regulatory procedures in Canada. The minimal use of the three secondary avenues discussed in this section are utilized in conjunction with the avenues of influence presented in sections 6.1 and 6.2 to diagnose a very weak degree of regulatory capture by data brokers in Canada.

6.3.1: Committee Hearings

Another avenue of influence available to firms is testifying in front of House and/or Senate Standing Committees. A House Committee is a working group comprised of a limited number of MPs who review in detail and improve bills or study issues related to the committee's mandate. To complete their studies, Committees hear testimony from private citizens, experts, representatives of organizations, public servants and Ministers to testify which allows the witnesses to set out their points of view and gives Members of Parliament (MP) the opportunity to ask questions (House of Commons n.d.). Witnesses appearing before a standing committee are typically proposed by a committee member, however, they can also be invited to appear by the committee or proactively notify the committee of their desire to testify (Bosc and Gagnon 2017). Testifying in front of a committee allows witnesses to critique or complement the bill being studied, share their expertise on the subject, discuss how the bill helps or hinders the group they represent, and propose amendments. Through this avenue, firms and industry associations can promote their business interests without increasing their lobbying expenditures.

For the Standing Committee on Industry and Technology's (INDU) study of Bill C-27 there is minimal evidence of data brokers using this avenue of influence to advance their interests. The only data brokers that testified on Bill C-27 were digital age data brokers and, more specifically Big Tech firms. On February 7th, 2023, representatives from Amazon Web Services, Google, Meta and Microsoft testified in front of the INDU committee on Bill C-27. These Big

Tech firms specifically participated INDU's study of AIDA and did not testify at hearings that focused exclusively on the CPPA. The representative Google did however discuss the CPPA and privacy more broadly in their opening statement. According to Jeanette Patell (2023), director of government affairs and public policy at Google Canada, "Google has long championed smart, interoperable and adaptable data protection regulations" and supports the government's efforts to modernize Canada's privacy regulatory framework but also believes consent provisions in the CPPA should be "both clarified and tailored to more consequential activities" and that a more consistent federal definition of minors is needed.

The absence of data broker participation in House committee hearings on Bill C-27 mirrors can be attributed to two interrelated factors. First, with CPPA not imposing stringent restrictions on the commercial uses of personal information and the inclusion of the legitimate interest clause there was no need for data brokers to propose amendments that align with their business interests. For Daniel Konikoff (2023) of the CCLA, Bill C-27 is "porous with these exemptions and exceptions, and these gaps come at the expense of people's privacy", all of which benefit firms and their data monetization practices. Conversely, Sara Clodman (2023) of the Canadian Marketing Association, whose members include data brokers such as Epsilon, Ipsos, Loblaw, Meta, the Trade Desk, urged "the speedy adoption of the CPPA". Moreover, since Bill C-27 did not grant the OPC the power to issue binding orders, levy monetary penalties or regulate using tripartism, there was minimal need for data brokers to testify in order to protect their business practices.

Second, testifying at committee would draw unwanted attention to the data broker industry from the government and the public, both of which would be antithetical to the industry's clandestine operation. For firms and industries whose business practices are the target of a specific bill, testifying in front of a House or Senate committee and proposing amendments can be a promising avenue for firms to shape narratives around policy issues and redirect or weaken the legislation. The same applies for submitting written briefs to the Committee in lieu or in addition to testifying. This avenue becomes especially useful if the industry and issue area are of high political salience and if it is utilized in conjunction with domestic lobbying.

6.3.2: Business and Industry Associations

One way in which firms and industries can advance their interests and exert their influence is through business and/or industry associations. Membership in these associations enables firms to advance their interests collectively and with additional financial resources. Business associations such as the Canadian Chamber of Commerce and the Business Council of Canada focus on issues that impact the overall economy and promote policies that support business opportunities and growth. Conversely industry associations such as the Canadian Bankers Association and the Insurance Bureau of Canada are more narrowly focused and advocate for policies that support their respective industries. By leveraging their collective resources business and industry associations can influence policies and shape regulations in ways that benefit their members. If this formal lobbying results in policies being continuously redirected from the public to the private interests, then a diagnosis of strong regulatory capture can be given. However, for data brokers there is no dedicated industry association that advocates for and/or lobbies on behalf of their collective interests.

The absence of a data broker industry association can be attributed to four factors. First, since Canada’s patchwork privacy regime favors the business practices of data brokers and promotes a self-regulating tech sector, there is minimal need for these firms to form an industry association to advance their collective interests. Second, with the varying data monetization practices of traditional and digital age data brokers it would be challenging for one association to represent the diverse needs of these firms. Third, since data brokers do not self-identify as such an industry specific association would draw clear boundaries around the types of firms that comprise the data broker industry and thus, expose the true size and scale of the industry. Lastly, a data broker industry association that lobbies on behalf of its members would expose their business practices to the public and the government. Despite the absence of an institutional arrangements through which data brokers can collectively deploy their business power, data brokers are members of associations representing marketing and advertising firms.

With over 700 leading media companies, brands, agencies and technology firms, the IAB “promotes the value of the interactive advertising industry to legislators and policymakers” (IAB n.d.). Some notable members of the IAB that can be found on the California’s registry and the list of data brokers presented in Chapter 4 are 33Across, Acxiom, Data Axle, Experian, illumin (formerly AcuityAds), LiveRamp, Oracle and Outbrain. Despite the size of the IAB, the formal lobbying activity of this association is rather limited. In Canada, the IAB has not formally lobbied on issues related to privacy and access to information since 2018 and in the U.S., the lobbying expenditures for the IAB on issues surrounding consumer product safety and computers and information technology in 2023 were only \$560,000 (USD) (OpenSecrets 2023). For data brokers that are members of the IAB, the benefit of their membership would not come from the association’s lobbying activities but from the opportunities to connect with other players in the advertising industry and thus, find new clients and/or business partners.

Another association in which data brokers participate is the Digital Advertising Alliance (DAA) which powers the AdChoice program, an online tool that allows consumers to know when their information is be collected and used for advertising. In Canada, the AdChoice program is run by the DAAC and requires participating firms to adhere to seven self-regulatory principles that include, transparency, consumer control, data security and accountability (DAAC 2022). Of the 71 companies

Table 6: Data Broker in the DAAC’s AdChoice Program

Participating Data Brokers	
Choreograph	Meta
Demandbase	Microsoft
Dianomi	NextRoll
Epsilon	Nexxen
Eyeota	OutBrain
FreeWheel (by Comcast)	ShareThrough
Google	StackAdapt
GroupM	Taboola
illumin (AcuityAds)	Teads
OwnerIQ	The TradeDesk
Knorex	The Weather Company

participating in the AdChoice program, 22 are data brokers (see Table 6). Despite the negative impact the self-regulatory principles would have on the data broker business model, being a member of the AdChoice program affords these data brokers the opportunity to shape the principles and the program. Since the DAAC promulgates voluntary standards across the advertising industry in Canada but does not involve any government oversight or a degree of

tripartism (Ayres and Braithwaite 1992) it cannot be considered a coregulatory scheme. With no external enforcement mechanism, data brokers participating in the AdChoice program can exercise their discursive power from the inside to frame ideas and shape the principles in ways that advance their interest over the interests of consumers.

6.3.3: Government Uses of Data Brokers

With this dissertation's focus on data and privacy rather than national security and party politics, the Canadian government and DPOHs have only been discussed in their capacities as regulators and legislators. However, since data brokers will sell, license and append data to any entity willing to pay, the Government of Canada and various political parties have employed the services of data brokers. The relationship between data brokers and Canada's federal political parties as well as security apparatus is an important avenue through which these firms can exercise their influence.

Federal political parties are in a unique position regarding their data collection and uses. Currently, neither PIPEDA nor the *Privacy Act* apply to political parties and *Canada Elections Act* allows parties to use data in accordance with the privacy policy's they draft themselves. For voters, this means parties can collect, utilize and append personal information in any way they see fit, including partnerships with data brokers. For example, at a House Committee hearing in 2018, the Conservative Party, Liberal Party and New Democratic Party each admitted to purchasing data from InfoCanada (now Data Axle) and Canada Post to append their lists of supporters (INDU 2018).³⁵ More recently, Environics, the "nation's leading data and analytics firm" launched VoterConnect, a powerful database that leverages fifteen custom-built socio-demographic Canadian voter segments and connects with other data tools such as Snowflake and DataBricks to "deliver tailored messages to the right voters" (Environics Analytics 2024). Lastly, for elections candidates partnering with digital age data brokers such as Facebook and Instagram to run paid political ads must also provide the platforms with personal information to target a specific demographic.

In terms of national security, the Royal Canadian Mounted Police (RCMP) have partnered with data brokers for a variety of policing purposes. Since 2015, the RCMP has been using private sector services to collect personal information from a range of sources, including: social media, forums, the dark web, location-based services and fee-for-access private databases (Phillip Dufresne 2024). Under Project Wide Awake the RCMP utilized Salesforces' Social Studio, Bable Street's Bable X, LifeRaft's Navigator and LTAS Technologies' WIST, to scrape social media accounts and publicly available information (Phillip Dufresne 2024). More specifically, the RCMP utilized Bable X to "design and initiate highly specific searches of publicly available information. Searches can be customized using geospatial and temporal parameters and be filtered by topics of interest and other inputs" (Royal Canadian Mounted Police 2022). The RCMP also used Clearview AI's facial recognition technology, for which it was investigated by the OPC and the provincial privacy regulators as the information scrapped by Clearview was deemed to be not 'publicly available' (Office of the Privacy Commissioner of Canada 2021). The use of data brokers for national security and law enforcement purposes is not unique to Canada. In the U.S., Immigration and Customs Enforcement (ICE) has partnered with LexisNexis and Equifax to circumvent

³⁵ The witnesses were: Trevor Bailey, Conservative Party of Canada; Michael Fenrick, Liberal Party of Canada and Jesse Calvert, NDP.

sanctuary policies and obtain real time information on incarcerations and jail bookings of migrants targeted for deportation (Bhuiyan 2022).

The utilization of data broker products and services by various actors across Canada's political system provides two additional insights on the industry's deployment of business power. First, the use of data broker data by Canada's security establishment and the federal political parties does not contradict the minimal awareness the legislative and regulatory branches of the Canadian government have on this industry. Instead, since no data broker classifies itself as a data broker it would be difficult for anyone without an intimate knowledge of the industry to know the true nature of the firms partnering with these government actors. By using terms such as 'data analytics firm' or 'software company', data brokers make it difficult to draw concrete lines on what types of firms are or are not considered data brokers and thus, maintain the shroud of secrecy that has protected their industry from regulation. This, however, does not negate or excuse the lack of due diligence prior to signing a contract with a data broker. Second, given the prioritization of national security over privacy and that political parties are not governed under PIPEDA, these two political actors can freely purchase the products and services of data brokers. With this mutually beneficial relationship data brokers in Canada, these firms can advance their interests quietly without lobbying by engaging with the behind-the-scenes decision makers.

This section has sought to present three additional avenues of influence through which firms, and more specifically data brokers can exercise their instrumental, structural and discursive forms of power. However, since Canada's privacy regime imposes weak restrictions on how firms' data collect and use data, data brokers have no need to utilize these channels to change a system that benefits their industry. Additionally, by using these avenues of influence data brokers risk exposing their industry's size and data monetization practices to regulators, legislators and Canadians who are largely unaware of the industry's existence and operations. Although data brokers have used committee hearings, business associations and government partnerships to advance their interests, the evidence of their influence through these channels minimal. Thus, with minimal use of the two primary avenues of influence discussed in sections 6.1 and 6.2, the three secondary avenues presented above point to a diagnosis of very weak regulatory capture.

Conclusion

Business power is a formidable force through which firms can exert disproportionate influence over policymakers and the policy making process to advance their interests. This can be done using instrumental, structural or discursive forms of power that firms can wield independently or collectively and can result in a strong degree of regulatory capture. As this chapter demonstrates, data brokers in Canada are minimally exercising their instrumental power to advance their interests, however, this industry is benefiting from structural and discursive forms of power. To arrive at this conclusion, this chapter presented and examined two primary and three secondary avenues of influence available to data brokers. The primary avenues included justifying data monetization practices, lobbying, and the secondary avenues encompassed testifying in Standing Committee hearings, creating and leveraging business associations, and partnering with the government. With minimal evidence supporting data brokers' uses of instrumental power, this chapter highlights how an industry can thrive without regulatory capture, resulting in the diagnosis of very weak regulatory capture, as these firms benefit from the structure of the capitalist system.

In order to diagnose capture, “a regulation, in law or application, is consistently or repeatedly directed away from the public interest and toward the interests of the regulated industry by the intent and action of the industry itself” (Carpenter and Moss 2013, p. 13). Based on examination of the five avenues of influence presented in this chapter there is insufficient evidence to demonstrate any consistent or repeated action by data brokers to direct a privacy law or regulation away from the public interest toward their private interest. Given the absence of data brokers employing their business power to weaken, shape or redirect a privacy regulation, a weak degree of regulatory capture can be diagnosed. The diagnosis of weak capture can be further downgraded to very weak given the minimal need for data brokers to repeatedly redirect regulations and exercise their power to advance their interests.

Through the presentation and examination of these avenues of influence, this chapter contends that the absence of regulation can be attributed to most regulators and legislators having a limited knowledge and/or awareness of the data broker industry and its operation in Canada opposed to a strong degree of regulatory capture. This conclusion is further supported by the fact that between 2006 and 2024 there were only eight mentions of data brokers and three mentions of selling data in the Hansards of the Parliament of Canada (House of Commons 2025). Given the limited Parliamentary discussions surrounding the operation of the global data broker industry in Canada, there is minimal need for these firms to lobby to advance their interests, weaken legislation or preserve their self-regulation. Additionally, this limited awareness also explains why policymakers have not addressed or been responsive to these firms monetize personal information, which further reduced the need for data brokers to utilize the three forms of business power to advance their interests.

In addition to the limited knowledge and awareness, this chapter also posits that by exercising their power, data brokers risk exposing their business practices to the regulators and legislators that are largely unaware of their industry’s existence and operation. Since the data broker industry operates in the shadows of the tech sector and advertising industry, lobbying, creating industry associations or testifying at Committee hearings would call attention to business practices of data brokers and expose the true size of the industry. Consequently, this could result in the political salience of their data monetization practices elevating from low to high. If this occurs, the data broker industry would come under increased regulatory scrutiny as it would be difficult for Canadian legislators and regulators to not act and protect the personal information and privacy of Canadian’s. However, thus far, this industry has managed to avoid garnering significant media attention as between 2020 and 2024 data brokers were only mentioned in eight articles published by the Globe and Mail and seven articles published by the Toronto Star and Post Media.

This chapter’s focus on the avenues through which data brokers can but largely do not exercise their business power to advance their interest has provided key insights that directly address and support this dissertation’s guiding research questions and central argument. The evidence presented and analyzed points to and supports the diagnosis of very weak regulatory capture by the data broker industry in Canada. With this diagnosis an alternative explanation (i.e. the government’s lack of knowledge on the data broker industry) for the absence of stringent privacy laws in Canada was presented in support of this dissertation’s central argument. Although there is a very weak degree of regulatory capture by data brokers, this chapter aimed to expose the ways in which this industry is benefiting from the subtlety of structural power afforded to them in a capitalist economic system and the inner workings of an industry that operates with minimal transparency.

Chapter 7: Conclusion

Introduction

As discussed throughout this dissertation's empirical chapters, the global data broker industry operates in the shadows and monetizes personal information using a variety of clandestine business practices. With minimal, albeit growing, attention to data brokers in policy circles, academia or mass media, this industry has been able to profit off personal information largely without interference. The widespread and pervasive collection and harvesting of personal information by data brokers has exacerbated individuals losing access to, control over and ownership of their data. In the wake of this growing privacy deficit, the twin objectives of this doctoral project have been to call attention to the global data broker industry and explain why this industry is under-regulated in Canada. From this starting point, a set of research questions was developed.

Guiding this dissertation are one primary and two secondary research questions. First, why can data brokers purchase, sell, license and/or append the personal information of Canadians notwithstanding national and sub-national privacy statutes that call for limitations on the collection, use and disclosure of personal information? Second, are data brokers, individually and/or collectively, exercising their business power through instrumental, structural and discursive channels to remain under-regulated? Third, is the business power and private interest influence of data brokers resulting in a strong or weak degree of regulatory capture?

This dissertation has argued that in pursuit of profits, innovation and economic growth, Canada's privacy regime has and continues to rely on quasi-self-regulation, non-prescriptive principles and weak limitations on the collection, use and disclosure of personal information, all of which permits and encourages the monetization of personal information by data brokers. As the government seeks to reap the benefits of free market capitalism, commercial interests have been placed ahead of consumer privacy. The prioritization of profits over privacy, coupled with the Canadian Government's limited knowledge of the data brokers industry, further contributes to the insufficient regulation of data brokers in Canada and minimizes the need for these firms to exercise their business power to advance their interests.

This concluding chapter is organized as follows. Section 7.1 highlights the primary empirical and theoretical contributions of the project as well as the evidence presented to support the main argument. Section 7.2 reiterates the value of employing a responsive regulatory approach to address the highly technical and evasive data broker industry in Canada. Lastly, Section 7.3 discusses avenues for future research on the global data broker industry.

7.1: Key Contributions and Answering the Research Questions

To address these research questions and support this central argument, data and evidence were collected from a variety of primary sources, including House Standing Committee transcripts, the privacy policies of B2C firms, lobbying registries, and privacy-related laws and regulations (such as PIPEDA, Bill C-27, and CASL). The first-hand knowledge and experiences of 14 elites obtained through semi-structured interviews were also presented as evidence throughout the empirical chapters. Using this data in conjunction with the theoretical approach presented in Chapter 3, this dissertation worked to identify how data brokers and Canada's privacy regime have enabled the under-regulation of this industry. In doing so, this dissertation has made several novel contributions to the study of data brokers and privacy, specifically in the Canadian context.

A key contribution of Chapter 4, which overviewed the global data broker industry, was the digital age data broker typology and the Data Brokers in Canada List. The digital age data broker typology differentiates between six types of data brokers that collect, trade, analyze and/or manage personal information to help individuals, legislators, regulators and academics identify firms that are monetizing personal information beyond strictly selling, licensing or appending data (i.e. traditional data brokers). This typology also contributes to the literature on data brokers and privacy, as future research can now differentiate between various types of marketing and advertising-oriented data brokers and thus, generate more specific insights on their privacy-protecting and/or violating business practices. To begin uncovering the size, scale and scope of the global data broker industry in Canada, I created the Data Brokers in Canada List (see Appendix A). This list identifies over 150 traditional and digital age data brokers and includes the data brokers' names, classification and headquarters.

The novel digital age data broker typology and data broker list in Chapter 4 drew attention to a clandestine industry that harvests vast amounts of personal information without detection. Together, these findings can be utilized by academics and policymakers to increase the effectiveness of privacy laws in protecting personal information when it is utilized by domestic and international data brokers. Additionally, Chapter 4 partially satisfied the primary research question of this doctoral project. Since data brokers do not self-identify as such (CIPPIC 2018a), it is not possible to regulate or monitor an industry whose members and business practices are not clearly defined. Thus, without a clear understanding of the types of firms that comprise this industry and their data monetization practices, data brokers will continue to be underregulated in Canada.

To further answer the first research question and start addressing the secondary questions, Chapter 5 identified three elements of Canada's privacy regime that contribute to the ongoing under-regulation of the data broker industry. First, Canada's complex patchwork of federal, provincial and industry-specific privacy statutes lack harmonization, makes compliance for firms challenging and imposes increased transaction costs on firms for compliance. This patchwork can result in firms complying with the least restrictive law or gambling with noncompliance, both of which fail to safeguard the personal information of Canadians. Second, PIPEDA's vague, non-prescriptive and quasi-self-regulatory nature affords firms a great deal of discretion in justifying collection purposes and determining reasonability. The novelty of this contribution arises from the conclusion that data brokers can then use this discretion and quasi-self-regulation to make their business practices PIPEDA-compliant and avoid regulatory scrutiny. Lastly, Canada's weak complaint-based enforcement regime is not responsive to how data brokers exploit the grey areas of privacy statutes or their highly technical and clandestine data harvesting techniques.

Together, the empirical contributions of Chapter 5 also worked to advance the literature on privacy and data brokers. By focusing on data brokers in Canada, this chapter expanded these two bodies of literature to an industry and country that have not received adequate scholarly attention. Moreover, by joining the literature on privacy with the literature on data brokers, this chapter was also able to identify gaps across Canada's patchwork privacy regime that enable the widespread collection and monetization of personal information. For the literature on privacy and privacy in Canada, these grey areas are not exclusive to data brokers and can be exploited by firms across a myriad of industries operating in Canada. The empirical contributions of this chapter also expand

the literature on private interest influence. Together, the quasi-self-regulation, grey areas and general gaps of Canada's privacy regime greatly reduce the need for firms and/or various cooperative arrangements to exercise business power when it comes to privacy laws and regulations.

To answer the three research questions and advance the central argument of this dissertation, Chapter 6 identified two primary and three secondary avenues of influence through which data brokers can exercise their business power. The combination of these five avenues of influence and minimal use of these channels by data brokers to advance their private interests was utilized to diagnose a very weak degree of regulatory capture by the data broker industry in Canada.

The first primary avenue of influence presented in this chapter was a set of predetermined economic assumptions that align corporate and government interests and minimize the need for data brokers to exercise their structural and discursive power to shape narratives and create markets. The notion of consumer rationality, firms having ownership over personal information, and the reliance on self-regulation to promote innovation are all entrenched features of capitalist economic systems and the regulation of big tech. Thus, it is unnecessary for data brokers to reshape ideas on why it is beneficial for consumers to disclose their personal information (discursive power) or work to create new markets through which they can monetize personal information (structural power). The second primary avenue of influence examined was formal registered data broker lobbying (instrumental power). The original examination of the formal lobbying activities of data brokers in the U.S. and Canada in Chapter 6 found minimal evidence of these firms exercising their instrumental power. The presentation of data brokers' uses of instrumental power expands the literature on business power and capture theory to an industry that has not been discussed. In doing so, Chapter 6 lays the foundation for future research into the lobbying activities and regulatory capture of data brokers and helps support the diagnosis of very weak regulatory capture.

Regarding the secondary avenues, Chapter 6 identified government contracts, testifying at standing committee hearings and industry associations. Through these three secondary avenues, data brokers could exercise their instrumental, structural and discursive power to individually or collectively weaken or shape privacy laws, policies and regulations. However, despite some examples of government contracts, mainly for elections and national security, there is no data broker-specific industry association in Canada, nor are these firms, aside from Big Tech platforms, testifying at committee hearings related to privacy. With the five avenues of influence being minimally used by data brokers to redirect regulations, in law or application, away from the public interest, Chapter 6 diagnosed a very weak degree of regulatory capture by data brokers. It is through the combination of these avenues, and more specifically, the overall absence of private interest influence, that the diagnosis of very weak regulatory capture was given.

The explanations for the absence of private interest influence presented across Chapter 6 and this dissertation were twofold. First, lobbying, testifying or creating industry associations risk exposing the data broker industry to regulators and legislators who have limited knowledge of this industry's operations. Second, since Canada's privacy regime favours the data broker industry, there is minimal need for these firms to exercise their power to shape, redirect or weaken privacy

laws. For the literature on business power and the theory of regulatory capture, this finding highlights the importance of not taking the absence of instrumental business power and a weak degree of capture at face value, as industry can survive without capture and benefit from structural power. Additionally, the diagnosis of a very weak degree of regulatory capture by the data broker industry in Canada also highlights a shortcoming of capture theory: that while it is useful to establish more rigorous criteria to identify strong regulatory capture, it is too narrow an approach to assess the possibility that the industry may achieve its interests by not exercising instrumental power but rather by benefitting from the structural power conferred on it by the properties of capitalism.

For Carpenter and Moss (2013, p. 13) regulatory capture “is the result or process by which regulation, in law or application, is consistently or repeatedly directed away from the public interest and toward the interests of the regulated industry by the intent and action of the industry itself.” In articulating such a precise and explicit definition of capture, Carpenter and Moss have necessitated a rigorous diagnosis of capture that inadvertently excludes more implicit forms of capture that are still hazardous. By setting a high bar for diagnosing capture, Carpenter and Moss also prevent singular attempts to weaken or redirect laws, policies and/or regulations from being diagnosed as capture.

Additionally, with this stringent definition of regulatory capture, Carpenter and Moss also point to the importance of public interest. In instances where the public has limited knowledge on a specific issue area, it is difficult to clearly define public interest and thus, identify when regulations are intentionally being redirected. To overcome the challenge of defining the public interest vis-à-vis privacy and an industry that is not public-facing, I, as the primary researcher, defined the Canadian public’s interest as the desire to be let alone. In this view, privacy and the public interest are the freedom from uses of personal data beyond their original purposes and the freedom to control how this data is used and by what entities. It is important to note that it is not the only version of the public interest. There can be a public interest in privacy as a fundamental human right that is essential for autonomy and democracy, and privacy for groups that is not reducible to the individuals of the group, as well as an interest in the use of personal data, for instance in exchange for free goods and services or public health. However, for this project’s use of Carpenter and Moss’s definition and diagnosis of capture, public interest is the desire to be let alone.

A compounding challenge that was highlighted in this dissertation is when the government defines the public interest and then drafts laws and regulations that favour private interests. For example, PIPEDA, the very law that “recognizes the right of privacy of individuals with respect to their personal information” simultaneously recognizes “the need of organizations to collect, use or disclose personal information” (Part 1, s.3). Bill C-27, the proposed update to PIPEDA that was intended strengthen Canada’s privacy regime, also contained provisions, such as the legitimate interest clause (s. 18(3)), that would have made it easier for firms to collect, use and monetize personal information. Additionally, since states in a capitalist system are dependent on firms for investments and revenues, it may be unnecessary for firms to repeatedly exercise their business power to redirect or weaken a regulation that, from the outset, favours industry interests.

For the global data broker industry in Canada, it is evident that these firms need not rely on capture to remain under-regulated as they benefit from the properties of the capitalist system that prioritize profit-making, self-regulation and economic growth (structural and discursive power). With this conclusion, this dissertation highlights the value in treating regulatory capture as an important question regarding how firms exercise their business power when two dimensions of that power, structural and discursive, are produced, in part, by the features of a capitalist economic system. Thus, this dissertation's diagnosis of a very weak degree of regulatory capture by data brokers is largely attributed to the specific requirements set out by Carpenter and Moss's definition, as well as the conclusion that an industry can not only survive but also thrive without capture.

With this dissertation's focus on the under-regulated global data broker industry in Canada, several contributions to the study of regulation more broadly were also made. First, the empirical findings of this dissertation highlighted the complexities associated with regulating technologies in the digital age. For the OECD (2025, p. 26), "Governments regulate for people by improving safety and reducing harm as well as by ensuring prosperity." With food safety, the harms, such as illness, are immediate and tangible. Conversely, with digital technologies, the harms can be intangible, intertemporal and rapidly evolving. For regulators and legislators, improving safety, reducing harms and ensuring prosperity is increasingly complex, and these challenges are further exacerbated by the knowledge gap between regulators, legislators and the digital technologies they seek to regulate.

Second, this dissertation expanded the understanding of regulation as both a mechanism to mitigate harms and a tool to promote innovation. The dual function of regulation thus attempts to strike a balance between consumer protection and business interests. Even though regulations are created to reduce harms and improve safety, legislators and regulators can and do tip the balance in favour of business interests. This can be done covertly or overtly. In both instances, it is imperative to investigate the role of influence. A related tertiary contribution to the study of regulation is that the absence of business power can be just as telling as the presence of business power. Whether that be industry associations lobbying or individual firms inviting a DPOH to a sporting event, these actors have the means to advance their interests if a given regulatory environment is inhospitable for their business practices. Thus, interrogating the contributing factors for the absence of business power can assist in identifying the weaknesses and gaps of both legislation and regulation that fail to improve safety, reduce harms and ensure prosperity.

7.2: Responsive Regulation in Canada

As of April 2025, there is no proposed private sector privacy law that seeks to modernize and/or replace PIPEDA. Previous attempts to repeal and/or update parts of PIPEDA have been unsuccessful. Focusing on Bill C-27, these failures can be divided into two broad categories. First, the death of Bill C-27 may be attributed to the dissolution of Parliament; however, before the prorogation, the bill was on the trajectory of failure as the legislative process was plagued by the three acts under one bill (CPPA, AIDA and PIDTA), a business-oriented consultation process, an apathetic and uncooperative Minister and ongoing delays at the committee stage. The second failure is associated with the text of Bill C-27. The inclusion of the legitimate interest clause, the absence of stronger enforcement powers for the OPC, and the creation of the tribunal based on Ministerial recommendations all work to promote profits at the expense of privacy.

Since responsive regulation encourages and requires continuous improvement in discovering lower-cost ways to achieve regulatory goals and better outcomes, (Braithwaite 2012), it is imperative for any future iteration of C-27 or new privacy bill to draw lessons from past successes and failures. To address and overcome these past failures, this section outlines six legislative recommendations that, based on responsive regulation, can be employed to address the under-regulated global data broker industry in Canada. Recommendations one through three are focused on affording individuals more control over their personal information, while recommendations four through six are centered around strengthening the OPC.

First, any forthcoming federal private sector privacy law should prioritize harmonization and interoperability with existing provincial statutes that set a high standard for privacy. To do so, the Fair Information Practice Principles should be prescriptive. As seen throughout Chapter 5, the non-prescriptive principles afford firms too much discretion to self-justify their data collection and consent practices. Additionally, these principles also leave a number of grey areas that can be easily exploited by data brokers who rely on highly technical and clandestine techniques to harvest and monetize personal information. Instead of providing firms with an exception for obtaining consent, as was the case in Bill C-27, thereby permitting the widespread collection and use of personal information, a new privacy law must ensure that innovation and profits are not prioritized over privacy. To do so, privacy as a fundamental right should be included in the text of the bill, not the preamble, from the outset.

Second, firms must be required to list all business partners, third parties and contractors with which they disclose the zero- and first-party information of their customers in their privacy policy. The firms should also be required to list what personal information is being disclosed and for what purposes, as well as obtain meaningful consent prior to transferring the data. This requirement would increase the transparency around the downstream industries that purchase products from data brokers, as well as the firms that enable and assist the operations of the global data broker industry. In doing so, this requirement would help reduce the information asymmetries between firms and individuals in terms of privacy trade-offs. Determining which data brokers and third parties are collecting and processing their personal information, as well as for what purposes, is a complicated and arduous task that most individuals would not have the time or knowledge to complete. Thus, by providing individuals with these lists, they can make more informed choices before accepting all cookies or agreeing to the terms of service. Additionally, this recommendation would assist individuals in obtaining their personal information from data brokers and other related firms, as well as correcting any incorrect or inaccurate information. Alongside this recommendation, a future privacy law should also grant individuals a right to erasure.

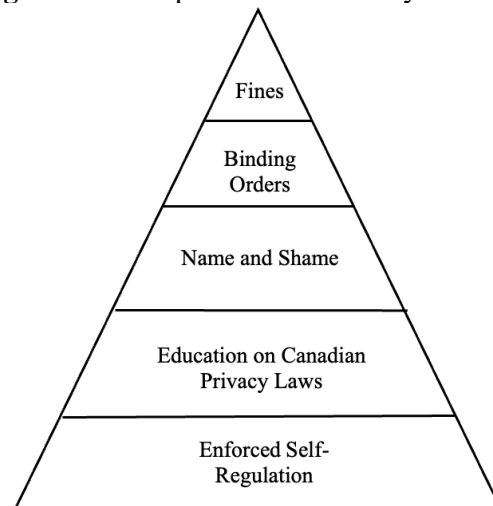
Third, any forthcoming privacy statute should provide individuals with the right to opt out of the sale of personal information without being denied access to the product and/or service. Similar to the provision in the California Consumer Privacy Act, firms operating in Canada should also be required to include a “Do Not Sell My Personal Information” link on their website and include specific details on how to exercise this right in their privacy policies. Since data brokers monetize personal information by selling, leasing, licensing, analyzing and/or appending data, this provision should be expanded to “Do Not Sell or Share My Personal Information.” Specifically, this requirement should exclusively be for secondary and/or tertiary data transfers that go beyond what is needed for the firm to provide the service (i.e. payment processing). This recommendation

works to regulate data brokers by reducing the supply of data flowing into this industry. In doing so, these firms will have fewer opportunities to monetize the personal information of consumers without their knowledge. With the legal right to prevent their personal information from being sold or shared, Canadians would be afforded more control over how their data is used and by which entities.

Turning to the OPC, the fourth recommendation is for the creation of a federal data broker registry that legally requires these firms to register with the OPC. As with the registries in California, Oregon and Texas, data brokers should be required to register annually and pay a registration fee. To account for Canada's federalist structure and the global nature of the data broker industry, the data broker registry should be national but also require the data brokers to specify the sub-national jurisdictions in which they operate. With a preexisting high degree of collaboration between the provincial and federal privacy regulators, creating one centralized data broker registry would eliminate the existence of multiple sub-national registries, as is the case in the U.S., which avoids imposing increased transaction costs on firms and double registration fees. To successfully capture the various types of data brokers discussed in Chapter 4, the privacy regulators must first develop and employ a comprehensive definition of a data broker. A useful starting point would be defining a data broker as any firm that harvests, collects, analyses, aggregates, sells, leases, licenses or appends zero through third-party personal information for profits.

The fifth recommendation would be affording the OPC stronger enforcement powers, such as the ability to issue binding orders and levy fines, tools to encourage compliance and the ability to create enforcement pyramids and enforcement strategies pyramids. Using the definition and registry presented in recommendation four, the privacy commissioners jointly work to categorize the firms on the registry based on their data monetization practices so that a typology, similar to the Digital Age Data Brokers typology in Chapter 4, can be created. In doing so, the OPC can then identify any ways in which each sub-category of data broker violates the clauses of Canada's new privacy statute, be responsive to emerging data monetization practices and develop tailored pyramids of supports and sanctions to address any contraventions. In creating these pyramids, the OPC should also engage in tripartism by partnering with various civil society organizations, such as the Canadian Civil Liberties Association (CCLA), to further strengthen the effectiveness of these regulatory pyramids and increase public awareness around the data broker industry. Figure 4 illustrates an enforcement pyramid that combines both supports and sanctions.

Figure 4: Example Enforcement Pyramid



Lastly, similar to the GDPR (Article 45), the OPC should conduct adequacy assessments for the jurisdictions in which data brokers transfer, store and analyze Canadian personal information and make this information publicly available. Moreover, as with the Digital Services Act (Article 2), which applies to intermediary services operating outside the EU, the OPC should

also require adequacy assessment for the jurisdictions in which data brokers and their business partners operate, regardless of geographic location. For countries such as the U.S., this assessment should be done at the sub-national level, as there is no federal private sector privacy law. For jurisdictions with an adequate level of protection, the OPC can review the privacy laws and regulations every three years. If the data is being transferred to a jurisdiction that offers a lower level of protection than provided in any new federal privacy act, the OPC should identify the weaknesses that can lead to privacy violations. If these gaps are minor, the OPC can work with the privacy authority of said jurisdiction to remedy the situation. Conversely, if the gaps are significant, the OPC should prevent any Canadian personal information from being transferred and/or processed in that jurisdiction until an adequate level of privacy protections is provided. Sanctions in the form of monetary penalties should also be in place if a firm transfers data to a jurisdiction without an adequate level of protection.

For any future private sector privacy law that the Canadian government aims to enact, these six recommendations offer a useful starting point for implementing a responsive regulatory approach. This approach, along with the recommendations discussed above, can offer Canadians increased control over their personal information, especially for individuals with limited time to determine which data brokers are harvesting and monetizing their personal information. Furthermore, employing a responsive regulatory approach will strengthen the enforcement powers of the OPC and allow regulators to identify and respond to the ways in which data brokers develop and deploy new data harvesting and monetization techniques.

The six recommendations discussed in this section are not exclusively applicable in the Canadian context. One of the benefits of responsive regulation is its usefulness for regulating rapidly evolving industries across a variety of political systems. For other jurisdictions, both national and sub-national, with outdated private sector privacy laws and weak enforcement regimes that also have an under-regulated data broker industry, these recommendations can easily be adjusted and implemented. More broadly, responsive regulation can also be adopted in jurisdictions with strong privacy laws and enforcement regimes, such as in Europe with the GDPR and the Digital Services Act, as tripartism, continually improving regulations and mixing punishments with persuasions are all useful tools for regulating rapidly evolving industries. From Big Pharma to Big Tech, a responsive regulatory approach can empower regulators, safeguard individuals and curb the non-compliant behaviour of firms.

7.3: Avenues for Future Research

As highlighted in section 7.1, this dissertation has made a number of relevant and original empirical and theoretical contributions to the study of the global data broker industry and its under-regulation in Canada. By examining how traditional and digital age data brokers monetize the personal information and attributes of Canadians for a variety of purposes, this doctoral project has shed light on an industry and country that have not received adequate attention across the literature. While this dissertation has offered numerous insights, this section outlines four areas for future research. These include investigating the regulation of financial information data brokers in Canada, data brokers and the provincial privacy laws, the informal avenues of influence available and used by data brokers, and the use of data governance frameworks.

Given the highly sensitive and personal information collected by financial information data brokers, a future area for research would be determining if and how these firms monetize the

personal information of Canadians. Some discussion surrounding the privacy implications of financial or risk mitigation data brokers in Canada has emerged (see Kanwal and Walby 2024); however, a comprehensive study similar to Leanne Rodrick's (2016) examination of the consumer credit data broker industry in the U.S. has yet to be undertaken in the Canadian context. It would be advantageous for future studies on financial and risk mitigation data brokers to evaluate the costs and harms experienced by Canadian consumers beyond data breaches.³⁶ Since credit reporting agencies are regulated both federally and provincially, a comparative case study analysis between and across these two levels would produce a novel contribution to the literature on data brokers and privacy.

A second area for future research relates to a more detailed examination of the efficacy of provincial privacy laws in regulating data brokers. Although the provincial laws are substantially similar to PIPEDA, they are not identical. Additionally, the provincial privacy regulators have a different set of enforcement powers to address noncompliance. For example, Quebec's Law 25 grants individuals' stronger privacy protections, such as requiring firms to obtain explicit consent and conduct privacy impact assessments. With the now apparent imbalance and lack of harmonization across Canada's privacy patchwork, it would be interesting for future research to determine if the personal information of individuals in certain provinces is less vulnerable to the data harvesting and monetization techniques of data brokers. This research could also investigate if data brokers are lobbying provincial regulators and legislators, or, if similar to the federal level, it is more advantageous for these firms not to formally lobby.

A third avenue for future research would involve identifying how data brokers exercise their business power outside of formal channels. Given the limitations of Canada's lobbying registry (discussed in Chapter 6), there are numerous informal avenues through which data brokers can engage with federal DPOHs without having to report that specific communication. This would require identifying key individuals within the data broker industry and determining if they are inviting DPOHs to dinner, sporting events or company parties. Access to Information (ATI) requests would be a useful starting point for collecting data on these types of informal interactions between firms and DPOHs. An analysis of these informal avenues could be conducted at both the federal and provincial levels. Provincially, it would be advantageous to examine the lobbying activities of both traditional and digital age data brokers in Québec, given the strength of Law 25.

Lastly, with this dissertation's focus on privacy statutes and regulations it would be beneficial for future research to examine the use of data governance frameworks, such as data trusts and DAOs (decentralized autonomous organizations), that allow innovative uses of data and address privacy concerns. Succinctly, a data trust is "an independent organization that serves as a fiduciary for the data providers and governs their data's proper use" (Zarkadakis 2020), and a DAO is a transparent and autonomous entity governed by blockchain-stored smart contract rules that enable member-driven governance (Gorman 2023). This line of inquiry should focus on assessing the feasibility of data trusts and DAOs for the global data broker industry, identifying which entity would oversee these governance frameworks, evaluating past use of these frameworks in other industries, and their practicality in affording consumer additional controls over how their data is collected, used and transferred.

³⁶ A notable example is the 2017 attack on Equifax Inc. that compromised the social insurance numbers and other identifying data of 19,000 Canadians (Office of the Privacy Commissioner of Canada 2019b)

Lastly, with this dissertation's focus on privacy statutes and regulations, it would be beneficial for future research to examine the use of data governance frameworks, such as data trusts and DAOs (decentralized autonomous organizations), that allow innovative uses of data and address privacy concerns. Succinctly, a data trust is "an independent organization that serves as a fiduciary for the data providers and governs their data's proper use" (Zarkadakis 2020), and a DAO is a transparent and autonomous entity governed by blockchain-stored smart contract rules that enable member-driven governance (Gorman 2023). This line of inquiry should focus on assessing the feasibility of data trusts and DAOs for the global data broker industry, identifying which entity would oversee these governance frameworks, evaluating past use of these frameworks in other industries, and their practicality in affording consumers additional controls over how their data is collected, used and transferred.

Conclusion

In closing, this dissertation sought to increase the transparency around the global data broker industry's operation in Canada. To do so, the types of personal information data brokers monetize, a digital age data broker typology was developed, over 150 data brokers operating in Canada were identified, and numerous examples of data brokers harvesting personal information were cited. With these empirical contributions, this dissertation aspired to inform individuals and regulators of the harms associated with this industry and increase the political salience of data brokers. Additionally, this dissertation worked to identify the regulatory and statutory gaps across Canada's privacy regime that fail to protect Canadian consumer data from data brokers. An original assumption was that data brokers are exercising their private interest influence to remain regulated; however, as discussed in Chapter 6, there is minimal evidence of data brokers lobbying or using their other forms of business power to advance their interests.

A primary objective of this dissertation was to explain why data brokers are underregulated in Canada. The theoretical and empirical contributions presented throughout this dissertation worked to support my central argument, which advances two explanations for the Government of Canada's insufficient regulation of data brokers. First, since data brokers do not self-identify as such, operate in the shadows and use highly technical data monetization techniques, the absence of regulation can be attributed to the Government of Canada's minimal knowledge of this industry's existence and operations. Second, to not stifle innovation and economic growth in the digital age, the Canadian government has sought to balance profits and privacy. However, through trade agreements, privacy laws and the alignment with corporate interests, firms have been encouraged to collect, use and transfer data across borders, all of which tips the scales in favour of profits. Together, these two factors have created an environment that affords consumers minimal privacy protections, permits data brokers to monetize personal information with limited government oversight and ultimately prioritizes profits over privacy.

Works Cited

- Aaronson, Susan Ariel. 2020. *Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves*. Centre for International Governance Innovation. <https://www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves/>.
- Aaronson, Susan Ariel, and Patrick Leblond. 2018. "Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO." *Journal of International Economic Law* 21(2): 245–72. doi:10.1093/jiel/jgy019.
- Acquisti, Alessandro. 2014. "The Economics and Behavioral Economics of Privacy." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, eds. Helen Nissenbaum, Julia Lane, Stefan Bender, and Victoria Stodden. Cambridge: Cambridge University Press, 76–95. doi:10.1017/CBO9781107590205.005.
- Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2020. "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age." *Journal of Consumer Psychology* 30(4): 736–58. doi:10.1002/jcpy.1191.
- Acquisti, Alessandro, and Jens Grossklags. 2005. "Privacy and Rationality in Individual Decision Making." *IEEE security & privacy* 3(1): 26–33. doi:10.1109/MSP.2005.22.
- Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016a. "The Economics of Privacy." *Journal of economic literature* 54(2): 442–92. doi:10.1257/jel.54.2.442.
- Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016b. "The Economics of Privacy." *Journal of Economic Literature* 54(2): 442–92.
- Acquisti, Alessandro, and Hal R. Varian. 2005. "Conditioning Prices on Purchase History." *Marketing Science* 24(3): 367–81. doi:10.1287/mksc.1040.0103.
- Acxiom. 2024. "What Is 2nd Party Data? Leverage More Customer Data to Achieve New Levels of Marketing Insight." *Acxiom*. <https://www.acxiom.com/second-party-data/> (July 18, 2024).
- Aguerre, Carolina. 2019. "Digital Trade in Latin America: Mapping Issues and Approaches." *Digital Policy, Regulation and Governance* 21(1): 2–18. doi:10.1108/DPRG-11-2018-0063.
- Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ko de Ruyter, and Martin Wetzels. 2015. "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness." *Journal of retailing* 91(1): 34–49. doi:10.1016/j.jretai.2014.09.005.
- Aïmeur, Esma, Gilles Brassard, and Muxue Guo. 2022. "How Data Brokers Endanger Privacy." *Transactions on Data Privacy* 15. <https://www.tdp.cat/issues21/tdp.a448a21.pdf>.

- Allen, Marshall. 2018. "Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates." *NPR*. <https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates> (March 20, 2025).
- Alphabet Inc. 2024. "Alphabet Inc. Form 10-K:" <https://abc.xyz/assets/43/44/675b83d7455885c4615d848d52a4/goog-10-k-2023.pdf>.
- Amazon Ads. "A Complete Guide to Media Buying." *Amazon Ads*. <https://advertising.amazon.com/library/guides/media-buying> (August 28, 2024a).
- Amazon Ads. "What Is AdTech and Why Is It Important?" *Amazon Ads*. <https://advertising.amazon.com/library/guides/what-is-adtech> (August 28, 2024b).
- Amo, Daniel, David Fonseca, Marc Alier, Francisco José García-Peñalvo, María José Casañ, and María Alsina. 2019. "Personal Data Broker: A Solution to Assure Data Privacy in EdTech." In *Learning and Collaboration Technologies. Designing Learning Experiences*, eds. Panayiotis Zaphiris and Andri Ioannou. Cham: Springer International Publishing, 3–14. doi:10.1007/978-3-030-21814-0_1.
- Andrew, Jane, and Max Baker. 2021. "The General Data Protection Regulation in the Age of Surveillance Capitalism." *Journal of Business Ethics* 168(3): 565–78. doi:10.1007/s10551-019-04239-z.
- Anshari, Muhammad, Mohammad Nabil Almunawar, Syamimi Ariff Lim, and Abdullah Al-Mudimigh. 2019. "Customer Relationship Management and Big Data Enabled: Personalization & Customization of Services." *Applied Computing and Informatics* 15(2): 94–101. doi:10.1016/j.aci.2018.05.004.
- Anupam Chander. 2017. "The Racist Algorithm?" *Michigan law review* 115(6): 1023–45.
- Arantes, Janine. 2024. "Educational Data Brokers: Using the Walkthrough Method to Identify Data Brokering by Edtech Platforms." *Learning, Media and Technology* 49(2): 320–33. doi:10.1080/17439884.2022.2160986.
- Arendt, Hannah. 1958. *The Human Condition*. Collector's ed. Chicago: University of Chicago Press.
- Arthur, Lisa. 2014. *Big Data Marketing: Engage Your Customers More Effectively and Drive Value*. Hoboken, New Jersey: John Wiley & Sons, Inc.
- Austen, Ian. 2022. "'A Mass Invasion of Privacy' but No Penalties for Tim Hortons - The New York Times." *The New York Times*. <https://www.nytimes.com/2022/06/11/world/canada/tim-hortons-privacy-data.html> (April 30, 2024).
- Austin, Lisa. 2015. "Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State." In *Law, Privacy and Surveillance in Canada in*

- the Post-Snowden Era*, University of Ottawa Press.
<https://www.jstor.org/stable/j.ctt15nmj3c.8?pq-origsite=summon> (April 4, 2023).
- Ayres, Ian, and John Braithwaite. 1992. *Responsive Regulation Transcending the Deregulation Debate*. New York: Oxford University Press.
- Azmeh, Shamel, Christopher Foster, and Jamie Echavarri. 2020. "The International Trade Regime and the Quest for Free Digital Trade." *International Studies Review* 22: 671–92.
- Bachechi, Chiara, Laura Po, and Federica Rollo. 2022. "Big Data Analytics and Visualization in Traffic Monitoring." *Big data research* 27: 100292-. doi:10.1016/j.bdr.2021.100292.
- Baldwin, Robert, Martin Cave, and Martin Lodge. 2011. *Understanding Regulation Theory, Strategy, and Practice*. 2nd ed. Oxford ; Oxford University Press.
- Balsillie, Jim. 2023. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts." <https://www.ourcommons.ca/DocumentViewer/en/44-1/INDU/meeting-90/evidence>.
- Bannerman, Sara, and Angela Orasch. 2020. "Privacy and Smart Cities: A Canadian Survey." *Canadian Journal of Urban Research* 29(1): 17–38.
- Barocas, Solon, and Helen Nissenbaum. 2014. "Big Data's End Run around Anonymity and Consent." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, eds. Helen Nissenbaum, Julia Lane, Stefan Bender, and Victoria Stodden. Cambridge: Cambridge University Press, 44–75. doi:10.1017/CBO9781107590205.004.
- Barth, Susanne, and Menno D. T. de Jong. 2017. "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review." *Telematics and Informatics* 34(7): 1038–58. doi:10.1016/j.tele.2017.04.013.
- Bauer, Matthias, and Hosuk Lee-Makiyama. 2014. "THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ECONOMIC RECOVERY." *European Center for International Political Economy* (3).
- Bélanger, France, and Robert E. Crossler. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS quarterly* 35(4): 1017–41. doi:10.2307/41409971.
- Bell, Stephen, and Andrew Hindmoor. 2015. *Masters of the Universe, Slaves of the Market*. Harvard University Press. <https://www.jstor.org/stable/j.ctvjhzsnh> (December 21, 2024).
- Bennett, Colin. 1991. "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s." *Science, Technology, & Human Values* 16(1): 51–69. doi:10.1177/016224399101600103.

- Bennett, Colin. 1996. "Rules of the Road and Level Playing-Fields: The Politics of Data Protection in Canada's Private Sector." *International Review of Administrative Sciences* 62(4): 479–91. doi:10.1177/002085239606200403.
- Bennett, Colin. 2020. "Stronger Privacy Enforcement Powers for the Privacy Commissioner." *Colin J. Bennett*. <https://www.colinbennett.ca/blog/stronger-privacy-enforcement-powers-for-canadaaes-privacy-commissioner-and-a-possible-rule-for-canadaaes-competition-bureau/> (May 29, 2024).
- Bennett, Colin. 2023. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts." <https://www.ourcommons.ca/documentviewer/en/44-1/INDU/meeting-92/evidence>.
- Bennett, Colin, and Charles Raab. 2003. *The Governance of Privacy: Policy Instruments in Global Perspectives*. Burlington, VT, USA: Ashgate.
- Bergemann, Dirk, and Alessandro Bonatti. 2019. "Markets for Information: An Introduction." *Annual Review of Economics* 11(1): 85–107. doi:10.1146/annurev-economics-080315-015439.
- BGR Government Affairs. 2023. "Lobbying Disclosure Registration: Snap Inc." <https://lda.senate.gov/filings/public/filing/f6638fd4-962c-4c9c-85ea-7084eb85ad5a/print/> (February 10, 2025).
- Bhuiyan, Johana. 2022. "US Immigration Agency Explores Data Loophole to Obtain Information on Deportation Targets." *The Guardian*. <https://www.theguardian.com/us-news/2022/apr/19/us-immigration-agency-data-loophole-information-deportation-targets> (January 29, 2025).
- Biden, Joseph. 2024. "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." *The White House*. <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/> (September 5, 2024).
- Black, Julia. 1996. "Constitutionalising Self-Regulation." *Modern law review* 59(1): 24–55. doi:10.1111/j.1468-2230.1996.tb02064.x.
- Blue Mountain Strategies. 2024. "Lobbying Disclosure Registration: Meta Platforms, Inc." <https://lda.senate.gov/filings/public/filing/4a207d72-f04b-4892-82b5-626b6d06a4ef/print/> (February 10, 2025).
- Booth, Barbara. 2024. "What Internet Data Brokers Have on You — and How You Can Start to Get It Back." *CNBC*. <https://www.cnbc.com/2024/10/11/internet-data-brokers-online-privacy-personal-information.html> (March 30, 2025).

- Borgesius, Frederik Zuiderveen, Jonathan Gray, and Mireille van Eechoud. 2015. "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework." *Berkeley Technology Law Journal* 30(3): 2073–2131. doi:10.15779/Z389S18.
- Bosc, Marc, and André Gagnon. 2017. *House of Commons Procedure and Practice*. Third. Éditions Yvon Blais.
- Boutilier, Alex. 2024. "RCMP Slammed for Private Surveillance Use to Trawl Social Media, 'Darknet' - National | Globalnews.Ca." *Global News*.
<https://globalnews.ca/news/10298074/rcmp-privacy-commissioner-report-social-media/>
 (April 30, 2024).
- Boyd, Danah, and Kate Crawford. 2012. "Critical Questions for Big Data." *Information, communication & society* 15(5): 662–79. doi:10.1080/1369118X.2012.678878.
- Bradford, Anu. 2019. *The Brussels Effect: How the European Union Rules the World*. New York, NY: Oxford University Press.
- Bradford, Laura, Mateo Aboy, and Kathleen Liddell. 2020. "COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes." *Journal of Law and the Biosciences* 7(1): lsaa034. doi:10.1093/jlb/lsaa034.
- Braithwaite, John. 2002. *Restorative Justice & Responsive Regulation*. Oxford ; Oxford University Press.
- Braithwaite, John. 2012. "The Essence of Responsive Regulation." *University of British Columbia law review* 44(3): 475–520.
- Brandimarte, Laura, and Alessandro Acquisti. 2012. "The Economics of Privacy." In *The Oxford Handbook of the Digital Economy*, eds. Martin Peitz and Joel Waldfogel. Oxford University Press, 0. doi:10.1093/oxfordhb/9780195397840.013.0020.
- Brandwatch. 2023. "10 Essential Methods for Effective Consumer and Market Research." *Brandwatch*. <https://www.brandwatch.com/blog/market-research-methods/> (August 26, 2024).
- "Breach of Personal Information Involving Cambridge Analytica and Facebook." 2018.
<https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-123/evidence>
 (January 29, 2025).
- Breckenridge, Adam Carlyle. 1970. *The Right to Privacy*. University of Nebraska Press.
- Brehmer, H Jacqueline. 2018. "Data Localization The Unintended Consequences Of Privacy Litigation." *American University Law Review* 67(3).
- Brockell, Gillian. 2018. "Perspective | Dear Tech Companies, I Don't Want to See Pregnancy Ads after My Child Was Stillborn." *Washington Post*.

- <https://www.washingtonpost.com/lifestyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/> (August 28, 2024).
- Bruno, Robert. 2000. "The Myth of the Powerless State." *Labor Studies Journal (Transaction Publishers)* 25(2): 129-.
- Burgess, Jean, Nicholas Carah, Daniel Angus, Abdul Obeid, and Mark Andrejevic. 2024. "Why Am I Seeing This Ad? The Affordances and Limits of Automated User-Level Explanation in Meta's Advertising System." *New Media & Society* 26(9): 5130–49. doi:10.1177/14614448241251796.
- Burri, Mira. 2017. "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation." *University of California, Davis Law Review* 51.
- Burri, Mira, and Rodrigo Polanco. 2020. "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset." *Journal of International Economic Law* 0(0): 1–34.
- Cadwalladr, Carole, and Emma Graham-Harrison. 2018. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (December 31, 2024).
- California Privacy Protection Agency. 2024. *Data Broker Registry*. State of California. https://coppa.ca.gov/data_broker_registry/ (January 16, 2025).
- Calo, Ryan. 2014. "Digital Market Manipulation." *The George Washington law review* 82(4): 995-.
- Cameron, Alex. 2023. "Privacy Legal Update: Recent & Upcoming Privacy Law Developments." Presented at the IAPP Canada Privacy Symposium.
- Campbell-Verduyn, Malcolm, Marcel Goguen, and Tony Porter. 2017. "Big Data and Algorithmic Governance: The Case of Financial Practices." *New political economy* 22(2): 219–36. doi:10.1080/13563467.2016.1216533.
- Carpenter, Daniel. 2013a. "Corrosive Capture? The Dueling Forces of Autonomy and Industry Influence in FDA Pharmaceutical Regulation." In *Preventing Regulatory Capture*, eds. Daniel Carpenter and David A. Moss. Cambridge University Press, 152–72. doi:10.1017/CBO9781139565875.011.
- Carpenter, Daniel. 2013b. "Detecting and Measuring Capture." In *Preventing Regulatory Capture: Special Interest Influence and How to Limit It*, eds. Daniel Carpenter and David A. Moss. Cambridge: Cambridge University Press, 57–68. doi:10.1017/CBO9781139565875.006.

- Carpenter, Daniel, and David Moss. 2013. "Introduction." In *Preventing Regulatory Capture: Special Interest Influence and How to Limit It*, eds. Daniel Carpenter and David A. Moss. Cambridge: Cambridge University Press. doi:10.1017/CBO9781139565875.
- Casalini, Francesca, and Javier López González. 2019. 220 *Trade and Cross-Border Data Flows*. . OECD Trade Policy Papers. doi:10.1787/b2023a47-en.
- Cavoukian, Ann, David Stewart, and Beth Dewitt. 2012. *Have It All - Protecting Privacy in the Age of Analytics*. Deloitte.
- Cecere, Grazia, Fabrice Le Guel, Matthieu Manant, and Nicolas Soulié. 2017. "The Economics of Privacy." In *The New Palgrave Dictionary of Economics*, London: Palgrave Macmillan UK, 1–11. doi:10.1057/978-1-349-95121-5_3058-2.
- Centre for Digital Rights. 2023. *Not Fit For Purpose – Canada Deserves Much Better*. <https://www.centrefordigitalrights.org/our-work/canada-privacy-regulation> (March 7, 2024).
- Cerny, Philip G. 2010. "The Competition State Today: From Raison d'État to Raison Du Monde." *Policy studies* 31(1): 5–21. doi:10.1080/01442870903052801.
- Cespedes, Frank V., and H. Jeff Smith. 1993. "Database Marketing: New Rules for Policy and Practice." *Sloan management review* 34(4): 7–22.
- Chandra, Shobhana, Sanjeev Verma, Weng Marc Lim, Satish Kumar, and Naveen Donthu. 2022. "Personalization in Personalized Marketing: Trends and Ways Forward." *Psychology & marketing* 39(8): 1529–62. doi:10.1002/mar.21670.
- CIPPIC. 2006. *On the Data Trail: How Detailed Information about You Gets into the Hands of Organizations with Whom You Have No Relationship*.
- CIPPIC. 2018a. *Back on the Data Trail: The Evolution of Canada's Data Broker Industry*. Canadian Internet Policy and Public Interest Clinic.
- CIPPIC. 2018b. "What Is a Data Broker?" *The Data Brokers Project*. <http://databrokers.cippic.ca/> (April 4, 2023).
- Ciuriak, Dan. 2018. *The Economics of Data: Implications for the Data-Driven Economy*. Centre for International Governance Innovation. <https://papers.ssrn.com/abstract=3118022> (September 25, 2024).
- Clodman, Sara. 2023. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts."
- Coglianesse, Cary, and Evan Mendelson. 2010. "Meta-Regulation and Self-Regulation." In *The Oxford Handbook of Regulation*, Oxford Handbooks in Business and Management, Oxford University Press. doi:10.1093/oxfordhb/9780199560219.003.0008.

- Cohen, Benjamin J. 2007. "The Transatlantic Divide: Why Are American and British IPE so Different?" *Review of International Political Economy* 14(2): 197–219.
- Competition Bureau. 2022. "False or Misleading Representations and Deceptive Marketing Practices." <https://competition-bureau.canada.ca/deceptive-marketing-practices/types-deceptive-marketing-practices/false-or-misleading-representations-and-deceptive-marketing-practices> (May 12, 2024).
- Competition Bureau Canada. 2020. "Facebook to Pay \$9 Million Penalty to Settle Competition Bureau Concerns about Misleading Privacy Claims." <https://www.canada.ca/en/competition-bureau/news/2020/05/facebook-to-pay-9-million-penalty-to-settle-competition-bureau-concerns-about-misleading-privacy-claims.html> (May 14, 2024).
- Constantiou, Ioanna D, and Jannis Kallinikos. 2015. "New Games, New Rules: Big Data and the Changing Context of Strategy." *Journal of Information Technology* 30(1): 44–57. doi:10.1057/jit.2014.17.
- Consumer Reporting Act*. 1990. <https://www.ontario.ca/laws/view> (May 12, 2024).
- Cooley, Thomas. 1880. *A Treatise on the Law of Torts, or, The Wrongs Which Arise Independent of Contract*. 2nd ed. Chicago: Callaghan & Co.
- Cote, Catherine. 2022. "How to Do Market Research for a Startup." *Business Insights Blog*. <https://online.hbs.edu/blog/post/how-to-do-market-research-for-a-startup> (August 26, 2024).
- Coutu, Sasha, and Jen Rees-Jones. 2024. "Canada's PIPEDA Remains 'Adequate' under the GDPR: What It Means for Business." *Dentons Data*. <https://www.dentonsdata.com/canadas-pipeda-remains-adequate-under-the-gdpr-what-it-means-for-business/> (May 29, 2024).
- Crain, Matthew. 2018. "The Limits of Transparency: Data Brokers and Commodification." *New Media & Society* 20(1). doi:10.1177/1461444816657096.
- Crawford, Kate. 2014. "When Big Data Marketing Becomes Stalking." *Scientific American*. <https://www.scientificamerican.com/article/when-big-data-marketing-becomes-stalking/> (April 4, 2023).
- Croft, Patti, and Catherine McNally. 2023. "What Is a Web Beacon and Why Should You Care?" *All About Cookies*. <https://allaboutcookies.org/what-is-a-web-beacon> (August 9, 2024).
- Culnan, Mary J., and Cynthia Clark Williams. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches." *MIS quarterly* 33(4): 673–87. doi:10.2307/20650322.
- Culpepper, Pepper. 2010. *Quiet Politics and Business Power: Corporate Control in Europe and Japan*. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511760716.

- Cutler, Claire. 2002. "Private International Regimes and Interfirm Cooperation." In *The Emergence of Private Authority in Global Governance*, eds. Rodney Hall and Thomas Biersteker. , 23–40. doi:10.1017/CBO9780511491238.003.
- Cutler, Claire, Virginia Haufler, and Tony Porter. 1999. "Private Authority and International Affairs." In SUNY series in global politics, Albany: SUNY Press.
- Cyphers, Bennett. 2020. "Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It." *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and> (March 7, 2024).
- DAAC. 2022. *The Canadian Self-Regulatory Principles For Interest-Based Advertising*. Digital Advertising Alliance of Canada. <https://assets.youradchoices.ca/pdf/principles/DAAC-AdChoices-Principles-English.pdf>.
- Dal Bó, Ernesto. 2006. "Regulatory Capture: A Review." *Oxford Review of Economic Policy* 22(2): 203–25. doi:10.1093/oxrep/grj013.
- Data Axle. 2024. "Interests and Behaviors." <https://platform.data-axle.com/people/docs/interests#behaviors> (July 17, 2024).
- Data Axle Canada. 2024. "Reach Your Canadian Audience." *Data Axle Canada*. <https://www.dataaxlecanada.ca/> (July 17, 2024).
- Databricks. 2023. "Data Marketplace." *Databricks*. <https://www.databricks.com/glossary/data-marketplace> (August 25, 2024).
- Datarade and Gravy Analytics by Unacast. 2024. "Audiences -- Interest-Based Targeting Audiences for the U.S. and Canada Built on Real-World Consumer Visits and Behavior." <https://datarade.ai/data-products/custom-mobile-audiences-segments-personas> (July 17, 2024).
- Datarade and Redmob. 2024. "Redmob: Consumer Behaviour Data - Global - 1.5B Devices, Real-Time Bidding Data." <https://datarade.ai/data-products/redmob-consumer-behaviour-data-global-1-5b-devices-real-redmob> (March 29, 2024).
- DeAngelo, Gregory, Adam Nowak, and Imke Reimers. 2018. "Examining Regulatory Capture: Evidence from the Nhl." *Contemporary Economic Policy* 36(1): 183–91. doi:10.1111/coep.12240.
- DeVries, Will Thomas. 2003. "Protecting Privacy in the Digital Age." *Berkeley Technology Law Journal* 18(1): 283.
- Digital Advertising Alliance of Canada. 2024. "Frequently Asked Questions." *AdChoices*. <https://about.youradchoices.ca/en/faq> (July 8, 2024).

- Digital Citizen and Consumer Working Group. 2021. *Privacy and Data Protection as Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration*. Global Privacy Assembly. <https://globalprivacyassembly.org/wp-content/uploads/2021/10/1.3h-version-4.0-Digital-Citizen-and-Consumer-Working-Group-adopted.pdf>.
- Dodge, Martin, and Rob Kitchin. 2005. “Codes of Life: Identification Codes and the Machine-Readable World.” *Environment and planning. D, Society & space* 23(6): 851–81. doi:10.1068/d378t.
- Dufresne, Philippe. 2023. “Privacy as a Fundamental Right in the Digital Age: Keynote Remarks at the 25th Annual Vancouver International Privacy & Security Summit (VIPSS).” https://www.priv.gc.ca/en/opc-news/speeches/2023/sp-d_20230224/ (April 30, 2024).
- Dufresne, Phillip. 2024. *Special Report to Parliament: Investigation of the RCMP’s Collection of Open-Source Information under Project Wide Awake*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/ (January 29, 2025).
- Elsig, Manfred, and Sebastian Klotz. 2021. “Digital Trade Rules in Preferential Trade Agreements: Is There a WTO Impact?” *Global Policy* 12(S4): 25–36. doi:10.1111/1758-5899.12902.
- Elvy, Stacy-Ann. 2018. “Commodifying Consumer Data in the Era of the Internet of Things.” *Boston College Law Review* 59(2): 423–522.
- Engstrom, David Freeman. 2013. “Corralling Capture.” *Harvard Journal of Law & Public Policy* 36(1): 31–40.
- Envionics. “PRIZM Segmentation System | Envionics Analytics.” *Default*. <https://envionicsanalytics.com/en-ca/data/segmentation/prizm> (August 26, 2024).
- Envionics Analytics. 2024. “Envionics Analytics Unveils ‘VoterConnect.’” *Default*. <https://envionicsanalytics.com/en-ca/resources/media-room/press-releases/2024/09/12/envionics-analytics-unveils--voterconnect> (January 29, 2025).
- Epsilon Marketing. 2023. “What Is First-, Second-, Third- and Zero-Party Data?” *Epsilon*. <https://www.epsilon.com/us/insights/blog/what-is-first-second-third-and-zero-party-data> (July 1, 2024).
- European Data Protection Board. “International Data Transfers.” https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en (September 26, 2024).
- Faucher, Guyllaume, and Stephanie Houle. 2023. *Digitalization: Definition and Measurement*. Bank of Canada. <https://www.bankofcanada.ca/2023/09/staff-discussion-paper-2023-20/> (August 28, 2024).

- Feenberg, Andrew. 2006. "What Is the Philosophy of Technology?" In *Defining Technological Literacy: Towards an Epistemological Framework*, ed. John Dakers. New York, UNITED STATES: Palgrave Macmillan US.
<http://ebookcentral.proquest.com/lib/mcmu/detail.action?docID=307740> (April 4, 2023).
- First Nations Information Governance Centre. 2023. *A First Nations Guide to The Personal Information and Electronic Documents Act (PIPEDA)*. https://fnigc.ca/wp-content/uploads/2023/07/Plain-Language-Guide-ENG_PROOF.pdf.
- Fox, Margalit. 2013. "Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83." *The New York Times*. <https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html> (April 4, 2023).
- Franklin Square Group, LLC. 2023. "Lobbying Disclosure Registration: Salesforce.Com Inc." <https://lda.senate.gov/filings/public/filing/5c877cae-a4bd-4536-8126-9083e66e20b4/print/> (February 10, 2025).
- French, Martin, and Torin Monahan. 2020. "Dis-Ease Surveillance: How Might Surveillance Studies Address COVID-19?" *Surveillance & Society* 18(1): 1–11.
doi:10.24908/ss.v18i1.13985.
- Fuchs, Doris. 2007. *Business Power in Global Governance*. Boulder: Lynne Rienner Publishers.
- Gao, Henry S. 2018. "Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation." *Legal Issues of Economic Integration* 45(1).
- Geist, Michael. 2015. *Law, Privacy, and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press. doi:10.26530/OAPEN_569531.
- Geist, Michael. 2023. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts." <https://www.ourcommons.ca/documentviewer/en/44-1/INDU/meeting-92/evidence>.
- Gellman, Robert. 2014. "Fair Information Practices: A Basic History." *SSRN Electronic Journal*. doi:10.2139/ssrn.2415020.
- Gilpin, Robert. 2001. *Global Political Economy: Understanding the International Economic Order*. Princeton, N.J: Princeton University Press.
- Gittens, J. Sébastien A., Stephen D. Burns, and Martin P. J. Kratz. 2018. "Understanding the GDPR: A Comparison Between the GDPR, PIPEDA and PIPA." *Lexology*. <https://www.lexology.com/library/detail.aspx?g=64796406-67e5-49e2-94b7-78a494f97311> (May 29, 2024).
- Glassdoor. 2024. "Salary: Privacy Officer in Canada 2024." *Glassdoor*. https://www.glassdoor.ca/Salaries/privacy-officer-salary-SRCH_KO0,15.htm (May 14, 2024).

- Goldstein, Kenneth. 2002. "Getting in the Door: Sampling and Completing Elite Interviews." *PS, political science & politics* 35(4): 669–72. doi:10.1017/S1049096502001130.
- Goldstone, Laura. 2023. "How Advertisers Are Leveraging Offline Data and Transparent Reporting to Power Campaigns." *Digiday*. <https://digiday.com/sponsored/how-advertisers-are-leveraging-offline-data-and-transparent-reporting-to-power-campaigns/> (March 31, 2025).
- Gorman, Ben. 2023. "What Is a Decentralized Autonomous Organization (DAO)?" *Avast*. <https://www.avast.com/c-what-is-dao>.
- Gratton, Eloïse, Elisa Henry, Francois Joli-Coeur, Denes Rothschild, and David Wood. 2020. *Marketing Your Business in Canada: Understanding the Laws and Risks Involved*. Borden Ladner Gervais.
- Gray, Liz. 2019. "Data-Driven Direct Marketing: Quality over Quantity." <https://databrokers.cippic.ca/2019/01/18/data-driven-direct-marketing-quality-over-quantity/> (April 4, 2023).
- Guilmain, Antoine. 2022. "The Privacy Officer: Every Organization Needs One Now in Québec." *Privacy and Access Council of Canada*. <https://pacc-ccap.ca/the-privacy-officer-every-organization-needs-one-now-in-quebec/> (May 13, 2024).
- Hall, Rodney, and Thomas Biersteker. 2002. 85 *The Emergence of Private Authority in Global Governance*. Cambridge: University Press. doi:10.1017/CBO9780511491238.
- Hallström, Jonas. 2022. "Embodying the Past, Designing the Future: Technological Determinism Reconsidered in Technology Education." *International journal of technology and design education* 32(1): 17–31. doi:10.1007/s10798-020-09600-2.
- Hayward, Robert. 1984. "Federal Access and Privacy Legislation and the Public Archives of Canada." *Archivaria*: 47–57.
- Heilweil, Rebecca. 2020. "Why Algorithms Can Be Racist and Sexist." *Vox*. <https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency> (April 4, 2023).
- Hofacker, Charles F., Edward Carl Malthouse, and Fareena Sultan. 2016. "Big Data and Consumer Behavior: Imminent Opportunities." *The Journal of consumer marketing* 33(2): 89–97. doi:10.1108/JCM-04-2015-1399.
- House of Commons. 2025. "Publication Search - Hansards." *Publication Search*. <https://www.ourcommons.ca/PublicationSearch/en/?targetLang=&Text=%22data+brokers%22&PubType=37&ParlSes=All&Topic=&Proc=&Per=&com=&oob=&PubId=&Cauc=&Prov=&PartType=&Page=1&RPP=15#> (March 1, 2025).

- House of Commons. “Guide for Witnesses Appearing Before House of Commons Committees.” *Parliament of Canada*. <https://www.noscommunes.ca/procedure/guides/witness-e.html> (February 2, 2025).
- Humby, Clive. 2021. “Clive Humby.” *University of Sheffield, School of Computer Science*. <https://www.sheffield.ac.uk/cs/people/academic-visitors/clive-humby> (July 31, 2024).
- Iacobucci, Edward. 2021. *Examining the Canadian Competition Act in the Digital Era*.
- Interactive Advertising Bureau. “IAB Our Story.” <https://www.iab.com/our-story/> (February 10, 2025).
- Intuit. 2024a. “Global Privacy Statement.” <https://www.intuit.com/privacy/statement/> (November 19, 2024).
- Intuit. 2024b. “Privacy and Security.” <https://www.intuit.com/privacy/data-usage/> (November 19, 2024).
- Kak, Amba, and Sarah Meyers-West. 2023. *AI Now 2023 Landscape: Confronting Tech Power*. AI Now Institute. <https://ainowinstitute.org/wp-content/uploads/2023/04/AI-Now-2023-Landscape-Report-FINAL.pdf>.
- Kammourieh, Lanah., Baar, Thomas., & Berens, Jos. (2017). Group Privacy in the Age of Big Data. In Linnet, Taylor, Luciano Floridi, & Bart van der Sloot (Eds.), *Group Privacy: New Challenges of Data Technologies* (1st ed.). Springer International Publishing.
- Kanwal, Rahul, and Kevin Walby. 2024. *Tracking the Surveillance and Information Practices of Data Brokers: A Report*. University of Winnipeg. <https://www.uwinnipeg.ca/caij/docs/reports/tracking-the-surveillance-and-information-practices-of-data-brokers.pdf>.
- Karbaliotis, Constantine. 2020. “What the Facebook-OPC Court Case Could Mean for Canadian Privacy Enforcement.” *IAPP*. <https://iapp.org/news/a/what-the-facebook-opc-court-case-could-mean-for-canadian-privacy-regulation> (May 29, 2024).
- Kim, Joanne. 2023. “Data Brokers and the Sale of Americans’ Mental Health Data.” *Duke Stanford Cyber Policy Program*. <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf>.
- Kitchin, Rob. 2014. *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. SAGE Publications Ltd. doi:10.4135/9781473909472.
- Konikoff, Daniel. 2023. “Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.”

- Kusserow, Richard. 2021. "Can a CEO Also Serve as a Compliance Officer?" *LinkedIn*. <https://www.linkedin.com/pulse/can-ceo-also-serve-compliance-officer-hon-richard-kusserow> (May 15, 2024).
- Laborde, Rebecca. 2020. "The Three V's of Big Data: Volume, Velocity, and Variety." *Oracle Health Science Blog*. <https://blogs.oracle.com/health-sciences/post/the-three-vx27s-of-big-data-volume-velocity-and-variety> (April 4, 2023).
- Laboucan, Amei-Lee. 2024. "What Is Indigenous Data Sovereignty and Why Does It Matter? - Beyond." *The University of British Columbia*. <https://beyond.ubc.ca/what-is-indigenous-data-sovereignty-and-why-does-it-matter/> (April 21, 2025).
- Laidlaw, Emily. 2021. *Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3790936.
- Laidler, John. 2019. "High Tech Is Watching You." *Harvard Gazette*. <https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/> (April 4, 2023).
- Lane, Julia, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, eds. 2014. *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge: Cambridge University Press. doi:10.1017/CBO9781107590205.
- Latto, Nica. 2020. "Data Brokers: Everything You Need to Know." *Avast*. <https://www.avast.com/c-data-brokers> (March 29, 2024).
- Laudon, Kenneth. 1996. "Markets and Privacy." *Communications of the ACM* 39(9): 92–104. doi:10.1145/234215.234476.
- Laudon, Kenneth C. 1996. "Markets and Privacy." *Communications of the ACM* 39(9): 92–105.
- Laufer, Robert S., and Maxine Wolfe. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory." *Journal of Social Issues* 33(3): 22–42. doi:10.1111/j.1540-4560.1977.tb01880.x.
- Lawford, John. 2023. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts."
- Leblond, Patrick. 2022. *A Digital Trade Strategy for Canada*. University of Ottawa. <https://www.ssrn.com/abstract=4261195> (September 5, 2024).
- Lee, Yi-Shan, and Roberto A. Weber. 2024. "Revealed Privacy Preferences: Are Privacy Choices Rational?" *Management Science*: mnsc.2022.00807. doi:10.1287/mnsc.2022.00807.

- Levin, Avner, and Mary Jo Nicholson. 2005. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground." *University of Ottawa Law & Technology Journal*. doi:10.32920/22227775.v1.
- Li, Shilei, Yang Liu, and Juan Feng. 2023. "Who Should Own the Data? The Impact of Data Ownership Shift from the Service Provider to Consumers." *Journal of Management Information Systems* 40(2): 366–400. doi:10.1080/07421222.2023.2196775.
- LiveRamp. 2022. "First-Party Data: What It Is, How to Use It, and Why It Matters Now More Than Ever." *LiveRamp*. <https://liveramp.com/explaining-first-party-data/> (July 18, 2024).
- Loi, M., & Christen, M. (2020). Two Concepts of Group Privacy. *Philosophy & Technology*, 33(2), 207–224. <https://doi.org/10.1007/s13347-019-00351-0>
- López González, Javier, and Marie-Agnes Jouanjean. 2017. 205 *Digital Trade: Developing a Framework for Analysis*. OECD. OECD Trade Policy Papers. doi:10.1787/524c8c83-en.
- Lotame. 2019. "What Is First-Party vs Third-Party Data: Definitions & Strategies." *Lotame*. <https://www.lotame.com/1st-party-2nd-party-3rd-party-data-what-does-it-all-mean/> (July 15, 2024).
- Lusha. 2024. "B2B Contact Database for Business & Corporate." *Lusha*. <https://www.lusha.com/data-attributes/> (August 6, 2024).
- Lyko, Klaus, Marcus Nitzschke, and Axel-Cyrille Ngonga Ngomo. 2016. "Big Data Acquisition." In *New Horizons for a Data-Driven Economy*, eds. Jose Maria Cavanillas, Wolfgang Wahlster, and Edward Curry. Springer Nature.
- MacLean, Jason. 2019. "Regulatory Capture and the Role of Academics in Public Policymaking: Lessons from Canada's Environmental Regulatory Review Process." *UBC Law Review* 52(2): 479.
- Makkai, Toni, and John Braithwaite. 1992. "In and out of the Revolving Door: Making Sense of Regulatory Capture." *Journal of Public Policy* 12(1): 61–78.
- Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15(4): 336–55.
- Manish, G. P., and Colin O'Reilly. 2019. "Banking Regulation, Regulatory Capture and Inequality." *Public Choice* 180(1): 145–64. doi:10.1007/s11127-018-0501-0.
- Margulis, Stephen. 1977. "Conceptions of Privacy: Current Status and Next Steps." *Journal of social issues* 33(3): 5–21. doi:10.1111/j.1540-4560.1977.tb01879.x.
- Martin, Kirsten. 2020. "Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms." *Business ethics quarterly* 30(1): 65–96. doi:10.1017/beq.2019.24.

- Massoc, Elsa. 2019. "Taxing Stock Transfers in the First Golden Age of Financial Capitalism: Political Salience and the Limits on the Power of Finance." *Socio-Economic Review* 17(3): 503–22. doi:10.1093/ser/mwx039.
- Mayer-Schönberger, Viktor, and Kenneth Cukier. 2014. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Reprint edition. Boston: Harper Business.
- McAfee, Andrew, and Erik Brynjolfsson. 2012. "Big Data: The Management Revolution." *Harvard Business Review*. <https://hbr.org/2012/10/big-data-the-management-revolution> (April 4, 2023).
- McClelland, Colin. 2021. "Data Brokers Are Tracking You — and Selling the Info." *Financial Post*. <https://financialpost.com/technology/data-brokers-are-tracking-you-and-selling-the-info> (April 4, 2023).
- McEvoy, Michael. 2023. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts." <https://www.ourcommons.ca/documentviewer/en/44-1/INDU/meeting-104/evidence>.
- McPhail, Brenda. 2023. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts." <https://www.ourcommons.ca/documentviewer/en/44-1/INDU/meeting-92/evidence>.
- Meltzer, Joshua. 2015. "The Internet, Cross-Border Data Flows and International Trade." *Asia & the Pacific Policy Studies* 2(1): 90–102. doi:10.1002/app5.60.
- Meltzer, Joshua. 2019. "Governing Digital Trade." *World Trade Review* 18(S1): S23–48. doi:10.1017/S1474745618000502.
- Meta Platforms, Inc. 2024. "Meta Platforms, Inc. Form 10-K." <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/c7318154-f6ae-4866-89fa-f0c589f2ee3d.pdf>.
- Milosevic, Theo, and Ellie Marshall. 2020. "A Call for Clarity: Ontario's Disjointed Privacy Class Actions and the Need for Privacy Law Reform." *The Canadian Class Action Review* 16(1): 127. <https://openurl.ebsco.com/contentitem/gcd:146163454?sid=ebsco:plink:crawler&id=ebsco:gcd:146163454> (May 12, 2024).
- Ministry Public and Business Service Delivery. 2021. *The Consumer Reporting Act – Proposals Under Consideration for Providing Access to Security Freezes, Credit Scores and Reports*.
- Moore, Roy L., Michael D. Murray, and Kyu Ho Youm. 2021. "Right of Privacy." In *Media Law and Ethics*, New York, NY: Routledge.

- Mukunda, Keshav. 2024. "Indigenous Data Sovereignty." *Simon Fraser University Library*. <https://www.lib.sfu.ca/help/publish/research-data-management/indigenous-data-sovereignty> (April 21, 2025).
- Mumford, Lewis. 1961. "History: Neglected Clue to Technological Change." *Technology and culture* 2(3): 230–36. doi:10.2307/3101022.
- Narayanan, Arvind, and Vitaly Shmatikov. 2010. "Myths and Fallacies of 'Personally Identifiable Information.'" *Communications of the ACM* 53(6): 24–26. doi:10.1145/1743546.1743558.
- National Assembly of Québec. 2021. *An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information*.
- Nesvetailova, Anastasia, and Ronen Palan. 2020. *Sabotage: The Hidden Nature of Finance*. First edition. New York: PublicAffairs.
- Obar, Jonathan A. 2022. "Defining and Assessing Data Privacy Transparency: A Third Study of Canadian Internet Carriers." *International journal of communication (Online)* 16: 1688-.
- O'Brien, David M. 1979. *Privacy, Law, and Public Policy*. New York, N.Y: Praeger.
- OECD. 1980. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." <https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm> (March 7, 2022).
- OECD. 2002a. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (September 1, 2024).
- OECD. 2002b. *OECD Reviews of Regulatory Reform: Canada 2002*. OECD. https://www.oecd.org/en/publications/oecd-reviews-of-regulatory-reform-canada-2002_9789264199095-en.html (April 17, 2025).
- OECD. 2025. *OECD Regulatory Policy Outlook 2025*. OECD. https://www.oecd.org/en/publications/2025/04/oecd-regulatory-policy-outlook-2025_a754bf4c.html.
- Office of the Commissioner of Lobbying of Canada. 2024. *Annual Report 2023-24*. Office of the Commissioner of Lobbying of Canada. <https://lobbycanada.gc.ca/media/1mikgudy/annual-report-2023-24-final-en.pdf>.
- Office of the High Commissioner for Human Rights. 2022. "Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns." *United National Human Rights*. <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report> (June 14, 2023).

- Office of the Privacy Commissioner of Canada. 2007. “Report of Findings: Privacy Commissioner of Canada v. SWIFT.” https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2007/swift_rep_070402/ (May 28, 2024).
- Office of the Privacy Commissioner of Canada. 2009. “Complaint under PIPEDA against Accusearch Inc., Doing Business as Abika.Com.” https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/2009_009_rep_0731/ (May 28, 2024).
- Office of the Privacy Commissioner of Canada. 2011. “Policy Position on Online Behavioural Advertising.” https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/bg_ba_1206/ (November 2, 2024).
- Office of the Privacy Commissioner of Canada. 2014. “Data Brokers: A Look at the Canadian and American Landscape.” https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/db_201409/#fn4 (July 15, 2024).
- Office of the Privacy Commissioner of Canada. 2018a. “Guidelines for Obtaining Meaningful Consent.” https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ (May 29, 2024).
- Office of the Privacy Commissioner of Canada. 2018b. “PIPEDA Requirements in Brief.” https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ (May 2, 2024).
- Office of the Privacy Commissioner of Canada. 2018c. “Summary of Privacy Laws in Canada.” https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/ (May 2, 2024).
- Office of the Privacy Commissioner of Canada. 2018d. “Who We Are.” <https://www.priv.gc.ca/en/about-the-opc/who-we-are/> (May 2, 2024).
- Office of the Privacy Commissioner of Canada. 2019a. “411Numbers Ceases Practice of Removing Information for a Fee.” <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-005/> (May 28, 2024).
- Office of the Privacy Commissioner of Canada. 2019b. “PIPEDA Findings #2019-001: Investigation into Equifax Inc. and Equifax Canada Co.’s Compliance with PIPEDA in Light of the 2017 Breach of Personal Information.” <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/> (March 30, 2025).
- Office of the Privacy Commissioner of Canada. 2020. “Provincial Laws That May Apply Instead of PIPEDA.” <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the->

- personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/ (May 4, 2024).
- Office of the Privacy Commissioner of Canada. 2021. *Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information Du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*. Office of the Privacy Commissioner of Canada. <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/> (January 29, 2025).
- Office of the Privacy Commissioner of Canada. 2023a. "Announcement: OPC to Investigate ChatGPT Jointly with Provincial Privacy Authorities." https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230525-2/ (March 31, 2025).
- Office of the Privacy Commissioner of Canada. 2023b. "Submission of the Office of the Privacy Commissioner of Canada on the Competition Act Reform." https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_competition_230320/#fn12-rf (May 12, 2024).
- Office of the Privacy Commissioner of Canada. 2024. "2023-24 Survey of Canadian Businesses on Privacy-Related Issues." https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2024/por_2023-24_bus/ (May 13, 2024).
- Office of the Vermont Attorney General. 2019. "Data Brokers." <https://ago.vermont.gov/blog/2017/12/05/data-brokers> (March 17, 2025).
- O'Leary, Daniel. 2015. "Big Data and Privacy: Emerging Issues." *IEEE intelligent systems* 30(6): 92–96. doi:10.1109/MIS.2015.110.
- OpenSecrets. 2023. "Interactive Advertising Bureau Lobbying Profile." *OpenSecrets*. <https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2023&id=D000026636> (February 10, 2025).
- Oracle. "What Is a Data Management Platform (DMP)?" <https://www.oracle.com/ca-en/cx/marketing/data-management-platform/what-is-dmp/> (August 25, 2024).
- Oracle Digital Experience Agency, and Gray Kaiti. 2022. "7 Types of Customer Attributes for Segmentation & Personalization." <https://blogs.oracle.com/marketingcloud/post/types-of-customer-attributes-for-segmentation-personalization> (July 18, 2024).
- Palmatier, Robert W., and Kelly D. Martin. 2019. *The Intelligent Marketer's Guide to Data Privacy The Impact of Big Data on Customer Trust*. 1st ed. 2019. Cham: Springer International Publishing. doi:10.1007/978-3-030-03724-6.
- Patel, Jeanette. 2023. "Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts."

- Pelmorex Corp. “Privacy Policy for The Weather Network and Pelmorex Corp.” *Privacy & Cookie Policies*. <https://www.theweathernetwork.com/info/privacy-policy-global> (March 31, 2025a).
- Pelmorex Corp. “Products.” <https://www.pelmorexsolutions.com/products/> (March 31, 2025b).
- Pence, Harry. 2015. “Will Big Data Mean the End of Privacy?” *Journal of educational technology systems* 44(2): 253–67. doi:10.1177/0047239515617146.
- Peng, Shin-yi. 2023. “Digital Trade.” In *The Oxford Handbook of International Trade Law*, Oxford Handbooks, eds. Daniel Bethlehem, Donald McRae, Rodney Neufeld, and Isabelle Van Damme. Oxford, New York: Oxford University Press.
- Penney, Jonathon. 2022. “Canadian Privacy Law and the Post-War Freedom of Information Paradigm.” In *Research Handbook on Privacy and Data Protection Law*, eds. Gloria González, Rosamunde Van Brakel, and Paul De Hert. Cheltenham, UK: Edward Elgar Publishing.
- Pennington, Krisetn, and Lyndsay Wasser. 2020. “Privacy Penalties – Canadian Competition Bureau Wades Into Privacy Enforcement.” *McMillan LLP*. <https://mcmillan.ca/insights/privacy-penalties-canadian-competition-bureau-wades-into-privacy-enforcement/> (May 12, 2024).
- Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. “Privacy Concerns and Consumer Willingness to Provide Personal Information.” *Journal of Public Policy & Marketing* 19(1): 27–41.
- Poitras, Diane. 2023a. “Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.” <https://www.ourcommons.ca/documentviewer/en/44-1/INDU/meeting-104/evidence>.
- Poitras, Diane. 2023b. “Bill C-27, An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.” <https://www.ourcommons.ca/documentviewer/en/44-1/INDU/meeting-104/evidence>.
- Porter, Tony. 1999. “The Late-Modern Knowledge Structure and World Politics.” In *Approaches to Global Governance Theory*, SUNY series in global politics, eds. Martin Hewson and Timothy J. Sinclair. Albany, NY: SUNY Press.
- Porter, Tony, and Michael Webb. 2008. “Role of the OECD in the Orchestration of Global Knowledge Networks.” In *The OECD and Transnational Governance*, eds. Rianne Mahon and Stephen McBride. Vancouver: UBC Press.
- Posner, Richard. 1974. “Theories of Economic Regulation.” *The Bell Journal of Economics and Management Science* 5(2): 335–58. doi:10.2307/3003113.

- Posner, Richard. 2013. "The Concept of Regulatory Capture: A Short, Inglorious History." In *Preventing Regulatory Capture: Special Interest Influence and How to Limit It*, eds. Daniel Carpenter and David Moss. Cambridge: Cambridge University Press, 49–56. doi:10.1017/CBO9781139565875.005.
- Posner, Richard A. 1978. "The Right of Privacy." *Georgia Law Review* 12(3).
- PricewaterhouseCoopers. 2023. *2023 Canadian Digital Trust Insights*. PwC Canada. <https://www.pwc.com/ca/en/services/consulting/cybersecurity-privacy/digitaltrust-insights.html>.
- Privacy Act*. 1983. <https://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.html?wbdisable=false> (May 2, 2024).
- Qualtrics. "The 8 Types of Market Research." *Qualtrics*. <https://www.qualtrics.com/experience-management/research/market-research-types/> (August 26, 2024).
- Rahman, Mohd Nayyer, and Nida Rahman. 2022. "Exploring Digital Trade Provisions in Regional Trade Agreements (RTAs) in Times of Crisis: India and Asia-Pacific Countries." *Asia and the Global Economy* 2(2): 100036. doi:10.1016/j.aglobe.2022.100036.
- Regan, Priscilla. 2003. "Privacy and Commercial Use of Personal Data: Policy Developments in the United States." *Journal of Contingencies and Crisis Management* 11(1): 12–18. doi:10.1111/1468-5973.1101003.
- Reclaim. "Join Reclaim - Take Back What's Yours!" *Reclaim*. <https://www.reclaimyours.com> (March 31, 2025).
- Rieke, Aaron, Harlan Yu, David Robinson, and Joris von Hoboken. 2016. *Data Brokers in an Open Society*. Upturn. <https://issuelab.org/resources/35958/35958.pdf>.
- Roderick, Leanne. 2014. "Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry." *Critical Sociology* 40(5): 729–46. doi:10.1177/0896920513501350.
- Roderick, Leanne. 2016. "Governing Big Data: The Political Economy of Power, Knowledge and Consumer Finance in the Digital Age." Queen's University.
- Rostama, Guilda, and Teresa Scassa. 2023. "The Future of Data Protection Enforcement in Canada: Lessons from the GDPR." *Canadian Journal of Law And Technology* 21(1).
- Rostow, Theodore. 2017. "What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers." *Yale Journal of Regulation* 34(2). <https://www.yalejreg.com/print/what-happens-when-an-acquaintance-buys-your-data-a-new-privacy-harm-in-the-age-of-data-brokers/> (September 6, 2024).

- Royal Canadian Mounted Police. 2022. *Babel X Platform*. Government of Canada. <https://www.rcmp-grc.gc.ca/en/babel-x-platform> (January 29, 2025).
- Rozenshtein, Alan. 2024. "Interpreting the Ambiguities of Section 230." *Yale Journal on Regulation*. <https://www.yalejreg.com/bulletin/interpreting-the-ambiguities-of-section-230/> (December 31, 2024).
- Rubinfeld, Jed. 1989. "The Right of Privacy." *Harvard Law Review* 102(4). https://openyls.law.yale.edu/bitstream/handle/20.500.13051/806/Right_of_Privacy__The.pdf?sequence=2.
- Rudzewicz, Adam, and Anna Strychalska-Rudzewicz. 2021. "The Influence of Brand Trust on Consumer Loyalty." *EUROPEAN RESEARCH STUDIES JOURNAL* XXIV(Special Issue 3): 454–70. doi:10.35808/ersj/2439.
- Salesforce. "What Is a Customer Data Platform (CDP)?" *Salesforce*. <https://www.salesforce.com/marketing/data/what-is-a-customer-data-platform/> (August 25, 2024).
- Saniuk-Heinig, Cheryl. 2021. "50 Years and Still Kicking: An Examination of FIPPs in Modern Regulation." <https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation/> (May 2, 2024).
- Sauvé, Pierre, and Marta Soprana. 2020. "The Evolution of the EU Digital Trade Policy." In *Law and Practice of the Common Commercial Policy*, eds. Michael Hahn and Guillaume Vanderloo. Brill. doi:10.1163/9789004393417_013.
- Savoie, Alexandra, Maxime-Olivier Thibodeau, Miguel Bernal-Castillero, and Nancy Holmes. 2020. "Canada's Federal Privacy Laws." https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/200744E (April 4, 2023).
- Scassa, Teresa. 2019. "Moving on From the Ombuds Model for Data Protection in Canada." *Canadian Journal of Law And Technology* 17(1).
- Schmunk, Rhianna. 2024. "Lawsuit Claiming Flo Health App Shared Intimate Data with Facebook Greenlit as Canadian Class Action." *CBC News*. <https://www.cbc.ca/news/canada/british-columbia/flo-health-privacy-class-action-1.7137600> (April 30, 2024).
- Shaffer, Gregory. 2021. "Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience." *World Trade Review* 20(3): 259–81. doi:10.1017/S1474745621000069.
- Shopify. 2023. "What Is Media Buying? Overview and How It Works." *Shopify Blog*. <https://www.shopify.com/ca/blog/media-buying>.
- Simmons, Alistair. 2023. "Data Brokers and the Sale of Students' Data." *Duke Stanford Cyber Policy Program*. <https://techpolicy.sanford.duke.edu/wp->

content/uploads/sites/4/2023/07/Data-Brokers-and-the-Sale-of-Students-Data-Simmons-2023.pdf.

- Skinner, David. 2020. "Race, Racism and Identification in the Era of Technosecurity." *Science as culture* 29(1): 77–99. doi:10.1080/09505431.2018.1523887.
- Slane, Andrea. 2018. "Information Brokers, Fairness, and Privacy in Publicly Accessible Information." *The Canadian Journal of Comparative and Contemporary Law* 4.
- Slane, Andrea. 2021. "Privacy Protective Roadblocks and Speedbumps Restraining Law Enforcement Use of Facial Recognition Software in Canada." <https://papers.ssrn.com/abstract=4275241> (April 4, 2023).
- Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly* 20(2): 167–96. doi:10.2307/249477.
- Smith, Michael, and Marshall W. Van Alstyne. 2021. "It's Time to Update Section 230." *Harvard Business Review*. <https://hbr.org/2021/08/its-time-to-update-section-230> (December 30, 2024).
- Smith, Miriam. 2017. "Historical Trajectories of Influence in Canadian Politics." In *A Civil Society?*, University of Toronto Press, 33–70. doi:10.3138/9781487593667.002.
- Smyth, Sara. 2019. "The Facebook Conundrum: Is It Time to Usher in a New Era of Regulation for Big Tech?" *International Journal of Cyber Criminology* 13(2): 578–95.
- Spithoff, Sheryl, Jessica Stockdale, Robyn Rowe, Brenda McPhail, and Nav Persaud. 2022a. "The Commercialization of Patient Data in Canada: Ethics, Privacy and Policy." *Canadian Medical Association journal (CMAJ)* 194(3): E95–97. doi:10.1503/cmaj.210455.
- Spithoff, Sheryl, Jessica Stockdale, Robyn Rowe, Brenda McPhail, and Nav Persaud. 2022b. "The Commercialization of Patient Data in Canada: Ethics, Privacy and Policy." *CMAJ* 194(3): E95–97. doi:10.1503/cmaj.210455.
- Standing Committee on Industry and Technology. 2024a. "Number 135." <https://www.ourcommons.ca/Content/Committee/441/INDU/Evidence/EV13268216/INDUEV135-E.PDF>.
- Standing Committee on Industry and Technology. 2024b. "Number 146." <https://www.ourcommons.ca/Content/Committee/441/INDU/Evidence/EV13438092/INDUEV146-E.PDF>.
- State of Oregon. 2024. "Division of Financial Regulation : Data Broker Registry." <https://dfr.oregon.gov/business/licensing/data-broker-registry/Pages/index.aspx> (July 11, 2024).

- Statistics Canada. 2023. *Digital Supply and Use Tables, 2017 to 2020*. Government of Canada. <https://www150.statcan.gc.ca/n1/daily-quotidien/230725/dq230725a-eng.htm> (August 28, 2024).
- Stigler, George. 1971. "The Theory of Economic Regulation." *The Bell Journal of Economics and Management Science* 2(1): 3–21. doi:10.2307/3003160.
- Stigler, George. 1980. "An Introduction to Privacy in Economics and Politics." *The Journal of Legal Studies* 9(4): 623–44.
- Stoddart, Jennifer. 2005. *Cherry Picking Among Apples and Oranges : Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA - October 2005*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2005/omb_051021/ (May 28, 2024).
- Stopford, John M., Susan Strange, and John S. Henley. 1992. *Rival States, Rival Firms: Competition for World Market Shares*. Cambridge: University Press.
- Stouffer, Clare. 2023. "What Are Data Brokers? Tips to Keep Your Data Safe - Norton." *Norton*. <https://us.norton.com/blog/privacy/data-brokers> (March 31, 2025).
- Strandburg, Katherine J. 2014. "Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, eds. Helen Nissenbaum, Julia Lane, Stefan Bender, and Victoria Stodden. Cambridge: Cambridge University Press, 5–43. doi:10.1017/CBO9781107590205.003.
- Strange, Susan. 1988. *States and Markets*. New York: Basil Blackwell.
- Strange, Susan. 1991. "An Eclectic Approach." In *The New International Political Economy*, International political economy yearbook ; v. 6, eds. Craig Murphy and Roger Tooze. Boulder: Lynne Rienner Publishers.
- Strange, Susan. 1997. "Territory, State, Authority and Economy: A New Realist Ontology of Global Political Economy." In *The New Realism: Perspectives on Multilateralism and World Order*, International Political Economy Series, ed. Robert W. Cox. London: Palgrave Macmillan UK, 3–19. doi:10.1007/978-1-349-25303-6_1.
- Stratton Oakmont, Inc. v. Prodigy Servs.,* 1995. (New York Supreme Court).
- Suh, Jeongmeen, and Jaeyoun Roh. 2022. "The Effects of Digital Trade Policies on Digital Trade." *SSRN Electronic Journal*. doi:10.2139/ssrn.4073187.
- Sun, Ruoxi, and Minhui Xue. 2020. "Quality Assessment of Online Automated Privacy Policy Generators: An Empirical Study." In *Proceedings of the Evaluation and Assessment in Software Engineering*, , 270–75. doi:10.1145/3383219.3383247.

- Talagala, Nisha. 2022. "Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires." *Forbes*. <https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/> (July 31, 2024).
- Tansey, Oisín. 2007. "Process Tracing and Elite Interviewing: A Case for Non-Probability Sampling." *PS: Political Science & Politics* 40(4): 765–72. doi:10.1017/S1049096507071211.
- Tarnoff, Ben. 2018. "Big Data for the People: It's Time to Take It Back from Our Tech Overlords." *The Guardian*. <https://www.theguardian.com/technology/2018/mar/14/tech-big-data-capitalism-give-wealth-back-to-people> (April 4, 2023).
- Taylor, Curt. 2004. "Privacy and Information Acquisition in Competitive Markets." *IDEAS Working Paper Series from RePEc*. <https://search.proquest.com/docview/1698154841?pq-origsite=primo> (April 5, 2023).
- Taylor, Linnet, Luciano Floridi, and Bart van der Sloot. 2017. "Introduction: A New Perspective on Privacy." In *Group Privacy: New Challenges of Data Technologies*, Philosophical Studies Series, 126, Cham: Springer International Publishing. doi:10.1007/978-3-319-46608-8.
- Texas Secretary of State. 2024. "Data Brokers." <https://www.sos.state.tx.us/statdoc/data-brokers.shtml> (March 17, 2025).
- Therrien, Daniel. 2021. *Projecting Our Values into Laws: 2020-2021 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/ar_202021/ (April 4, 2023).
- ThinkDataWorks. 2025. "Unlock Growth with Data Monetization." <https://www.thinkdataworks.com/solutions/data-monetization> (March 17, 2025).
- Tinuiti. 2021. "Data Types 101: What Are First Party, Second Party, and Third Party Data?" *Tinuiti*. <https://tinuiti.com/blog/privacy-prep/data-types/> (July 17, 2024).
- TransUnion. "Governing Legislation." <https://www.transunion.ca/about-us/governing-legislation> (May 12, 2024).
- Trudeau, Justin. 2021. "Minister of Innovation, Science and Industry Mandate Letter." <https://www.pm.gc.ca/en/mandate-letters/2021/12/16/minister-innovation-science-and-industry-mandate-letter> (May 23, 2024).
- Twetman, Henrik, and Gundars Bergmanis-Korats. 2020. *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

- United States Senate Committee on Commerce, Science and Transportation. 2013. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. Office of Oversight and Investigations Majority Staff. <https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577>.
- Varian, Hal. 1997. "Economics Aspects of Personal Privacy." In *Privacy and Self-Regulation in the Information Age*, United States Department of Commerce.
- Varian, Hal R. 2009. "Economic Aspects of Personal Privacy." In *Internet Policy and Economics: Challenges and Perspectives*, eds. William H. Lehr and Lorenzo Maria Pupillo. Boston, MA: Springer US, 101–9. doi:10.1007/b104899_7.
- Vedaschi, Arianna. 2018. "Privacy and Data Protection versus National Security in Transnational Flights: The EU–Canada PNR Agreement." *International data privacy law* 8(2): 124–39. doi:10.1093/idpl/ipy004.
- Velli, Federica. 2019. "The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements." *European Papers - A Journal on Law and Integration* 2019 4: 881894. doi:10.15166/2499-8249/325.
- Voss, W. Gregory. 2020. "Cross-Border Data Flows, the GDPR, and Data Governance." *Washington International Law Journal* 29: 485.
- de Vries, Marc. 2017. "Philosophy as Critique." In *Critique in Design and Technology Education*, Contemporary Issues in Technology Education, eds. Kay Stables and P. John Williams. Singapore: Springer Nature Singapore. doi:10.1007/978-981-10-3106-9.
- Wall, N., Reynolds, M., Jetté, R., & da Silva, G. (2024, September 24). *Federal Court of Appeal overturns Federal Court decision and finds that Facebook breached obligations under federal privacy law* | Insights | Torys LLP. <https://www.torys.com/en/our-latest-thinking/publications/2024/09/federal-court-of-appeal-finds-that-facebook-breached-obligations-under-federal-privacy-law>
- Warren, James, and Nathan Marz. 2015. *Big Data: Principles and Best Practices of Scalable Realtime Data Systems*. New York: Manning Publications Co. LLC.
- Warren, Samuel, and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4(5): 193–220.
- Weber, Rolf H. 2010. "Digital Trade in WTO-Law - Taking Stock and Looking Ahead." *Asian Journal of WTO & International Health Law and Policy* 5: 1.
- Weiss, Linda. 1997. "Globalization and the Myth of the Powerless State." *New Left review* 225(225): 3–27.
- Weiss, Linda. 2018. *The Myth of the Powerless State*. Ithaca, NY: Cornell University Press,. doi:10.7591/9781501711732.

- Westin, Alan F. 1967. *Privacy and Freedom*. 1st ed. New York: Atheneum.
- Winner, Langdon. 1980. “Do Artifacts Have Politics?” *Daedalus (Cambridge, Mass.)* 109(1): 121–36.
- Woll, Cornelia. 2013. “Lobbying under Pressure: The Effect of Saliency on European Union Hedge Fund Regulation.” *JCMS: Journal of Common Market Studies* 51(3): 555–72. doi:10.1111/j.1468-5965.2012.02314.x.
- World Bank Group. 2024a. “GDP (Current US\$) - United States, Canada.” *World Bank Open Data*. <https://data.worldbank.org> (January 24, 2025).
- World Bank Group. 2024b. “Population, Total - United States, Canada.” *World Bank Open Data*. <https://data.worldbank.org> (January 24, 2025).
- Wyatt, Sally. 2008. “Technological Determinism Is Dead; Long Live Technological Determinism.” In *The Handbook of Science and Technology Studies*, ed. Edward J. Hackett. United States: MIT Press.
- Yu, Shui. 2016. “Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data.” *IEEE access* 4: 2751–63. doi:10.1109/ACCESS.2016.2577036.
- Zarkadakis, George. 2020. “‘Data Trusts’ Could Be the Key to Better AI.” *Harvard Business Review*. <https://hbr.org/2020/11/data-trusts-could-be-the-key-to-better-ai> (April 15, 2025).
- Zingales, Luigi. 2013. “Preventing Economists’ Capture.” In *Preventing Regulatory Capture*, eds. Daniel Carpenter and David A. Moss. Cambridge University Press, 124–51. doi:10.1017/CBO9781139565875.010.
- Zittrain, Jonathan. 2014. “Facebook Could Decide an Election Without Anyone Ever Finding Out.” *The New Republic*. <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> (April 4, 2023).
- Zuboff, Shoshana. 2015. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of information technology* 30(1): 75–89. doi:10.1057/jit.2015.5.
- Zuboff, Shoshana. 2020. “Surveillance Capitalism | by Shoshana Zuboff.” *Project Syndicate*. <https://www.project-syndicate.org/magazine/surveillance-capitalism-exploiting-behavioral-data-by-shoshana-zuboff-2020-01> (March 29, 2025).

Appendix A: The Data Brokers in Canada List

Firm Name	Type of Data Broker	Headquarters	Website URL
33Across	AdTech, Marketplace, Traditional (Behavioural)	United States	https://www.33across.com
Acast	AdTech, Media Buying Network	Sweden	https://www.acast.com/
Activate International	Media Buying Network	United States	https://activeinternational.ca
Acxiom	Traditional (B2B and B2C)	United States	https://www.acxiom.com
AdButler	Traditional (B2B and B2C)	Canada	https://adbutler.com
Adform	AdTech, Media Buying Network	Denmark	https://site.adform.com/
Adobe Experience Cloud	AdTech, Marketplace	United States	https://business.adobe.com/ca/
Adroll	AdTech	United States	https://www.adroll.com/
adsquare	Traditional (Location)	Germany	https://adsquare.com
Adstra	Traditional	United States	https://adstradata.com
Aeroplan (Air Canada)	Loyalty Program and Rewards Credit Card	Canada	https://www.aircanada.com/ca/en/aco/home/aeroplan.html#/
Air Miles	Loyalty Program and Rewards Credit Card	Canada	https://www.airmiles.ca/
Alliant	Marketplace	United States	https://alliantinsight.com
Amazon Ad System	AdTech, Big Tech Platform, Loyalty Program Marketplace, Market Research	United States	https://advertising.amazon.ca
Amplitude	AdTech	United States	https://amplitude.com
Annalect	Traditional (Attributes)	United States	https://www.annalect.com
Audiencerate	AdTech	United Kingdom	http://www.audiencerate.com
AuDigent (Experian)	AdTech, Marketplace	United States	https://audigent.com
Basis	AdTech, Marketplace, Market Research.	United States	https://basis.com
Bombora	Traditional (B2B), Marketplace	United States	https://bombora.com
Branch	AdTech	United States	https://www.branch.io

Caddle	Market Research and Traditional (Attributes and Location)	Canada	https://getcaddle.com/
Cadent	AdTech, Marketplace, Traditional (Attributes and Location)	United States	https://cadent.tv
Choozle	AdTech, Marketplace, Media Buying Network	United States	https://choozle.com
Choreograph	Data provider for GroupM, a media buying network	United States	http://www.choreograph.com
Claritas	AdTech, Market Research, Traditional (B2C & B2B)	United States	https://claritas.com
Cognitiv	AdTech	United States	https://cognitiv.ai
Comscore	AdTech, Traditional (Attributes)	United States	https://www.comscore.com
Connected Interactive	AdTech and Traditional (Attributes and Location)	Canada	https://connectedinteractive.com
Contobox	AdTech, Marketplace	Canada	https://www.advertisers.contobox.com
Cossette	AdTech, Media Buying Network, Traditional	Canada	https://www.cossette.com/en/home
Criteo	AdTech, Media Buying Network	France	https://www.criteo.com
Cuebiq	AdTech, Traditional (Location)	United States	https://cuebiq.com/
Data Axle	Traditional	United States	https://www.data-axle.com/what-we-do/data-axle-canada/
Databricks	AdTech, Marketplace	United States	https://www.databricks.com/
DataFix	Traditional (Attributes and Location)	Canada	https://datafix.com/
Datarade	Marketplace	Germany	https://datarade.ai/
Datonic	Marketplace, Traditional (B2B and B2C)	United States	https://www.datonics.com
Demandbase	B2B Traditional	United States	http://www.demandbase.com
Dianomi	AdTech, Traditional	United Kingdom	https://www.dianomi.com
Dstillery	AdTech, Traditional	United States	https://dstillery.com/

Dynata	Market Research, Marketplace, Traditional (Attributes)	United States	https://www.dynata.com/
Environics	Market Research, Traditional	Canada	https://environicsanalytics.com/en-ca
Epitaph Group	AdTech, Traditional (Attributes)	Canada	https://dev.epitaphgroup.com/
Epsilon	Traditional and Media Buying Network	United States	https://www.epsilon.com/us
Equifax	Traditional (B2B, Credit, Attributes)	United States	https://www.equifax.com/business/data-assets/consumer-data/
Experian	Traditional (Credit Reporting, B2B Attributes)	Ireland	https://www.experian.com/business/solutions/data-solutions
Eyeota (Dunn & Bradstreet)	Data Marketplace and Traditional	Singapore	https://www.eyeota.com/
Foursquare	Traditional (Attributes, Location)	United States	https://foursquare.com
Freewheel	AdTech, Marketplace, Traditional (Attributes and Location)	United States	https://www.freewheel.com
Google/Alphabet	AdTech, Big Tech Firm	United States	https://www.google.com
Gravy Analytics by Unacast	Traditional (Location)	United States	https://www.unacast.com/
GroundTruth	Traditional (Location, attributes)	United States	https://www.groundtruth.com
Havas Edge	AdTech, Media Buying Network	United States	https://www.havasedge.com
Hilton Honours	Loyalty Program and Rewards Credit Card	United States	https://www.hilton.com/en/p/global-privacy-statement/
illumin (formerly AcuityAds)	AdTech, Media Buying Network	Canada	https://illumin.com/
Index Exchange	AdTech, Marketplace	Canada	https://www.indexexchange.com
Inuvo	AdTech, Traditional	United States	https://inuvo.com
iProspect	AdTech	United States	https://www.iprospect.com/
Ipsos	Market Research	France	https://www.ipsos.com/en-ca
IQM.com	AdTech, Traditional (Location and Attributes) Media Buying Network	United States	https://iqm.com
IQVIA	Traditional (Health), Marketplace	United States	https://www.iqvia.com/locations/canada

Kargo Global	AdTech, Traditional (Location and Attributes) Buying Network	United States	https://www.kargo.com
Kinesso	AdTech	United States	https://kinesso.com
Knorex	AdTech, Traditional (Location)	United States	https://www.knorex.com
LexisNexis	Traditional (B2B and B2C)	United States	https://www.lexisnexis.ca/en-ca/products/executive-dossier.page
LG Ad Solutions	AdTech	South Korea	https://lgads.tv
LinkedIn (Microsoft)	AdTech, Big Tech Firm	United States	https://ca.linkedin.com/
LiveIntent	Marketplace, Traditional	United States	https://www.liveintent.com
LiveRamp	AdTech, Traditional, Marketplace	United States	https://liveramp.com/
Loblaw Advance	Media Buying Network	Canada	https://www.loblawadvance.ca
Lotame	AdTech, Marketplace	United States	https://www.lotame.com/
Lytics	AdTech, Marketplace	United States	https://www.lytics.com/
M32 Connect	AdTech, Marketplace	Canada	https://m32connect.com
Magnite	AdTech, Marketplace	United States	https://www.magnite.com
Marriott Bonvoy	Loyalty Program and Rewards Credit Card	United States	https://www.marriott.com/loyalty.mi
Mediaocean	AdTech, Marketplace	United States	https://www.mediaocean.com
Merkle	Traditional (attributes)	United States	https://www.merkle.com/en.html
Meta Platforms	AdTech, Big Tech Firm	United States	https://about.meta.com/
Metro Moi	Loyalty Program and Rewards Credit Card	Canada	https://www.metro.ca/en/moi-program
Mplus	AdTech, Marketplace, Traditional (Attributes and Location)	Canada	https://mplustech.io
Native Touch	Market Research and Traditional (Attributes and Location)	Canada	https://nativetouch.com
Nativo	AdTech, Traditional (attributes and location)	United States	https://www.nativo.com
NextRoll	AdTech	United States	https://www.nextroll.com/
Nexxen	AdTech, Traditional	Israel	https://nexxen.com/
Nielsen	AdTech, Traditional, Marketplace	United States	https://www.nielsen.com

Nova	AdTech, Media Buying Network	Canada	https://www.createwithnova.com
Numeris	Market Research and Traditional (Attributes and Location)	Canada	https://numeris.ca
OpenX	Marketplace, Traditional	United States	https://www.openx.com
Outbrain and Teads	AdTech, Marketplace, Traditional (Attributes)	United States	https://www.teads.com/
OwnerIQ	Traditional, Marketplace	United States	https://www.owneriq.com
Patio	AdTech, Traditional (Location)	Canada	https://wearepatio.com
PC Optimum (Loblaw)	Loyalty Program and Rewards Credit Card	Canada	https://www.pcoptimum.ca/
PebblePost	Traditional (Location, attributes)	United States	https://www.pebblepost.com/privacy-policy/#privacy-brand
Performics	Market Research, Traditional	United States	https://www.performics.com
Perion	AdTech, Marketplace	United States	https://perion.com/
Perkopolis	Loyalty Program and Rewards Credit Card	Canada	https://www.perkopolis.com/
Petro-Points (Suncor)	Loyalty Program and Rewards Credit Card	Canada	https://www.petro-canada.ca/en/personal/discover-petro-points
Pheonix Group	Market Research	Canada	https://thephoenixgroup.ca
Pinterest	AdTech, Big Tech Firm	United States	https://ca.pinterest.com/
Plum (Indigo)	Loyalty Program and Rewards Credit Card	Canada	https://www.indigo.ca/en-ca/plum/
Quantcast	AdTech, Marketplace, Traditional	United States	https://www.quantcast.com/advertiser
RedMob	Traditional	Singapore	https://www.redmob.io/
Reklaim	Traditional (consumers sell their data)	Canada	https://www.reklaimyours.com
Resonate	Traditional (Attributes)	United States	http://www.resonate.com
Retargetly (Eplison)	AdTech, Traditional	United States	https://retargetly.com
Reveal Mobile	AdTech, Traditional (Location)	United States	https://revealmobile.com/
Roku	AdTech Data Provider/Big Tech Firm	United States	https://www.roku.com/en-ca/
Salesforce	AdTech, Marketplace	United States	https://www.salesforce.com/ca/
Samba.TV	AdTech, Traditional	United States	https://www.samba.tv/business

SAP Customer Data Platform	AdTech	Germany	https://www.sap.com/canada/products/crm/customer-data-platform.html
Scene+ (Cineplex and Scotiabank)	Loyalty Program and Rewards Credit Card	Canada	https://www.sceneplus.ca/
Seedtag	AdTech	United States	https://www.seedtag.com
Semasio (Samba TV)	AdTech, Traditional	United States	https://www.semasio.com
ShareThis	Traditional (B2B and B2C)	United States	https://sharethis.com
Sharethrough	AdTech	United States	https://www.sharethrough.com/
Snapchat	AdTech, Big Tech Firm	United States	https://www.snapchat.com/
Snowflake	Marketplace	United States	https://www.snowflake.com/en/
Sojern	Traditional (travel specific)	United States	https://www.sojern.com
Sonobi	AdTech, Traditional	United States	https://sonobi.com
Sovrn	AdTech, Traditional	United States	https://www.sovrn.com
Spotify	AdTech, Big Tech Firm	Sweden	https://open.spotify.com/
StackAdapt	AdTech, Marketplace	Canada	https://www.stackadapt.com
Student Price Card (SPC)	Loyalty Program and Rewards Credit Card	Canada	https://www.spccard.ca/
Taboola	AdTech	United States	http://www.taboola.com
Tapad	AdTech, Traditional	United States	https://www.tapad.com
Tealium	AdTech, Marketplace	United States	https://tealium.com
The Aber Group	Traditional (Consulting)	Canada	https://www.abergroup.com
The Trade Desk	AdTech, Marketplace	United States	https://www.thetradedesk.com
The Weather Network (Pellmorex Corp)	AdTech, Big Tech/Platform, Media Buying, Marketplace and Traditional	Canada	https://www.theweathernetwork.com/en
ThinkDataWorks	Marketplace	Canada	https://www.thinkdataworks.com/
Throttle	Traditional (health)	United States	https://www.throttle.io
TikTok (ByteDance)	AdTech, Big Tech Firm	China	https://www.tiktok.com/explore
Time and Space	Market Research and Traditional (Attributes)	Canada	https://timespacemedia.com
Touché	Marketplace, Traditional (Attributes)	Canada	https://www.touchemedia.com/en/

TransUnion	Traditional (Credit Reporting, Attributes)	United States	https://www.transunion.ca/product/aggregate-data
Triangle Rewards (Canadian Tire)	Loyalty Program and Rewards Credit Card	Canada	https://triangle.canadiantire.ca/en.html
Triton Digital	AdTech, Traditional	United States	https://tritondigital.com
Twilio Segment	AdTech, Marketplace	United States	https://segment.com/
V12 Marketing	Traditional	United States	https://v12marketing.com/
vdx.tv	AdTech	United States	https://www.vdx.tv/
Veeva Crossix	Traditional (Attributes and Health)	United States	https://www.veeva.com
Veraset	Traditional (Location)	United States	https://www.veraset.com/
Vericast	Traditional (Location, Attributes)	United States	https://www.vericast.com
Verticalscope	Traditional (Attributes)	Canada	https://www.verticalscope.com
Viant	AdTech, Marketplace	United States	https://www.viantinc.com
Vistar Media	AdTech, Marketplace	United States	https://www.vistarmedia.com
X	AdTech, Big Tech Firm	United States	https://x.com/?lang=en
Yahoo/Apollo Global Management	AdTech, Big Tech Firm	United States	https://ca.yahoo.com/
YellowPages	Traditional (Attributes and Location)	Canada	https://www.canada411.ca/
Zenith	Traditional (Attributes and Location)	United Kingdom	https://www.zenithmedia.com
Zeta	AdTech, Marketplace, Traditional	United States	https://zetaglobal.com/