Facebook and the Cambridge Analytica Scandal: Privacy and Personal Data Protections in Canada

by

Madeleine Le Jeune

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Communications

in

M.A. Communication

Carleton University
Ottawa, Ontario

Abstract

In 2018, the Cambridge Analytica/Facebook scandal made front page news, a data breach that allowed a third-party — Cambridge Analytica — access to the personal data of millions in several countries, including over 600,000 Canadians. The scandal brought to light privacy issues to regulator and in the aftermath, Canada conducted an investigation into this unsanctioned use of data. This thesis explores the details of that scandal and the resulting Canadian investigation by the Standing Committee on Access to Information, Privacy and Ethics (ETHI) and the Office of the Privacy Commissioner (OPC), as well as drawing on information from the 2009 Canadian Internet Policy and Public Interest Clinic (CIPPIC) complaint with the OPC, and the Broadcasting and Telecommunications Legislative Review (BTLR). These public records are used to provide a lens through which to explore topics of privacy and personal data protection in Canada and what they might mean in a social media platform context. This thesis explores the different regulatory mechanisms and makes some recommendations to improve personal data protection and privacy regulations in Canada, including behavioral and structural regulatory solutions that might mitigate similar such scandals in the future.

Acknowledgements

I wish to express my deepest gratitude to my wonderful thesis supervisor, Dr. Dwayne Winseck for his guidance and support, his knowledge and patience. Without his aid I would not have been able to complete my studies during such a challenging time.

I wish to show my gratitude to my lovely second reader, Dr. Tracey Lauriault, for her patience and understanding, insight and wisdom.

I wish to express my gratitude to Dr. Elizabeth Dubois, my external committee member, for her time and hard work on my thesis review and defence.

I wish to thank all the people whose assistance was a milestone in the completion of this thesis, including Dr. Chris Russill, who encouraged me to pursue a Masters, Bethany Berard, who advised me on my Masters application, Dr. Sandra Robinson, who inspired me to write on the topic of privacy and data protection, and Dr. Rena Bivens, our wonderful Graduate Advisor, and Laura Gareau, our phenomenal Graduate Administrator, both of whom supported me through challenging times.

I wish to acknowledge and thank the friends who supported me through the completion of my thesis.

I wish to extend a special thank you to my amazing sister, Dominique Le Jeune, for her unwavering belief in me as I completed my thesis, and to my life mentor, Andrea Dann, for always being an inspiration and guiding light.

Table of Contents

Chapter 1: Scandal! Cambridge Analytica and Its Use of Facebook Data

> *Social networking sites are a cultural phenomenon. In the last five years, the popularity of these sites has exploded, with millions of people around the world joining them to keep in touch with their friends and family and to meet new people. They represent a dramatic shift in the way people communicate, and their use raises interesting questions about long-held views on what it means to have a private life or a sense of "privacy" (CIPPIC, 2009, p. 6).*

1.1 Introduction

What does it mean to have personal privacy online in an age of increasingly all-encompassing social media giants? Moreover, what happens when one's privacy online is violated, and one's personal data are exposed and misused? These are some of the questions that governments struggled to address after March of 2018, when they learned that data brokerage company Cambridge Analytica and its parent company, the SCL Group, obtained unsanctioned[1] access to personal data of approximately 87 million

[1] The term "unsanctioned" is used here to refer to how Cambridge Analytica obtained the data that from Facebook via one application *This is Your Digital Life,* and reused them for a very different purpose. Cambridge Analytica used the data collected by *This is Your Digital Life* application as per the Facebook's

Facebook users, including over 600,000 people in Canada (ETHI, 2018, p. 9). This scandal ignited a flurry of activity by governments around questions of data protection and privacy, resulting in numerous public inquiries to assess how this unsanctioned use of data occurred and to mitigate this from occurring again (Winseck and Puppis, 2019). Many of the inquiries touched on a wide range of issues about social media, not only focusing on the Cambridge Analytica scandal, which resulted in broader investigations about social media in general. The United Kingdom, Canadian parliamentary inquiries, and the International Grand Committee led by the United Kingdom with representatives from 14 countries, however, focused solely on the scandal. These three inquiries provide a very detailed record of what happened, and in this thesis, I refer to these to inform my analysis. Prior to this scandal, governments had expressed concerns about privacy and data protection on social media platforms,[2] but the Cambridge Analytica scandal marked a tipping point in terms of social media regulation. The scandal exemplifies how the very foundation of social media platforms, the data that they collect, aggregate, and employ to provide tailored services to users and options for marketing to advertisers, can be exploited for less than positive and ethical goals (ETHI, 2018, p. vii). This is especially the case with respect to a platform as widely used and well-known as Facebook, which

---

usual platform business model that ended in 2015, where third-party applications were permitted to collect and retain user information. Cambridge Analytica however reused data collected for one purpose in unanticipated ways, beyond what would be the "reasonable expected use" by a third-party application.

[2] Some examples of growing government attention to social media regulation can be found in the 2009 CIPPIC Complaint with the Office of the Privacy Commissioner of Canada against Facebook (*https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/*), and the 2011 US Federal Trade Commission complaint against Facebook (*https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep*), as well as the EU Data Protection Authorities (DPAs) as part of European Data Protection Directive 95/46/EC (95 Directive) the predecessor to the EU's General Data Protection Regulation (GDPR) (Houser and Voss, 2019, p. 4).

currently holds approximately 74% market share of social media platforms on a worldwide basis.[3] In Canada, Facebook accounted for approximately 57% of unique monthly visitors to social media sites in 2019.[4] The revelation of this unsanctioned access and use of these social media data was the basis for governments to investigate and address how they might go about protecting the personal data and privacy of their citizens with regulations.

In Canada, "pursuant to its mandate under Standing Order 108(3)(*h*)(vii) and the motion adopted on Thursday, March 22, 2018," (ETHI, 2018, p.V) *The Standing Committee on Access to Information, Privacy and Ethics* (the ETHI Committee) investigated the breach, noting that the scandal "quickly brought to light much broader questions relating to the self-regulation of platform monopolies, the use of these platforms for data harvesting purposes, and their role in the spreading of disinformation and misinformation around the world" (ETHI, 2018, p. vii). The Facebook/Cambridge Analytica government inquiries related to this unsanctioned use of personal data led to more regulatory scrutiny of social media companies and other large internet companies. This scandal was a critical point for broader initiatives to create a new generation of internet regulation distinct from the relatively light-handed and industry-driven efforts that characterized internet governance since the 1990s[5].

---

[3] Social Media Stats Worldwide, August 2020, http://gs.statcounter.com/social-media-stats. This is down from the approximately 80% of social media market share that Facebook enjoyed in 2017.
[4] Canadian Media Concentration Research Project (CMCRP), *Media and Internet Concentration in Canada, 1984–2019,* (https://www.cmcrp.org/media-and-internet-concentration-in-canada-1984-2019/#audiovisual).
[5] Such light-handedness allowed internet giants to consolidate their power through acquisitions and mergers, with Facebook managing to "string together 67 unchallenged acquisitions, which seems impressive, unless you consider that Amazon undertook 91 and Google got away with 214" (Wu, 2018, p. 123).

In France, the *Facebook Mission* (May 2019) produced a report titled, "Regulation of social networks – Facebook experiment", which explored "a general framework for the regulation of the social networks, starting from the fight against online hatred" (Facebook Mission, 2018, p. 4). In the United Kingdom, the House of Lords Select Committee on Communications (2019) issued their report titled "Regulating in a digital world" that addressed the need to regulate social media platforms to ensure that users are protected. In the United States the Judiciary Committee (July 17, 2018) held several hearings to explore how social media platforms filter their content and how data is used in these environments. These are but a few of the responses from governments as seen in the Winseck and Puppis (2019) list that chronicled the growing number of public inquiries held around the world.

1.2 Facebook's "Data Breach" Scandal

In this thesis, I will employ the term data breach when speaking about the scandal, since it is the term most often used in the official records I reference, even though it is not technically a data breach.[6] A data breach in real terms is the stealing of data by a variety of means. In this case, the data were acquired via a third-party application – *This is Your Digital Life* by Aleksandr Kogan – that had the right to use these data when first accessed and collected. This makes the scandal more a case of unsanctioned use of personal data as the data were used for a purpose that they were unintended to, for which individuals did

[6] The European Union's General Data Protection Regulation (GDPR) defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to" personally identifiable information (PII). The Personal Information Protection and Electronic Documents Act (PIPEDA) defines breach of security safeguards as "the loss of unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA, or from a failure to establish those safeguards."

not agree to, and beyond the expectations of privacy users would normally have (Nissenbaum, 2004). Furthermore, Facebook had an agreement to share data via the *This is Your Digital Life* for the specific purpose of running the application on the Facebook platform and not for the one that Kogan ultimately used them for. As will be discussed in chapter 3, up until 2015, third-party applications had been mostly unrestricted, and there was unmonitored access to the social media user data by way of downloading the *This is Your Digital Life* application. Indeed, that was one of the main issues of a complaint filed back in 2009 by the Canadian Internet Policy and Public Interest Centre (CIPPIC) (CIPPIC, 2009, p. 38). Although Facebook's policy for third-party applications at the time stated that the data gathered by the application were not to be used beyond the intended use articulated in the application agreement, Facebook did not enforce this and user data were easily obtained and used by third-party applications (CIPPIC, 2009, pp. 41-42).

The Facebook and Cambridge Analytica data breach gained international attention on March 17, 2018, when The New York Times ran an article titled, *How Trump Consultants Exploited the Facebook Data of Millions.*[7] Based upon the testimony from a former whistleblowing employee of Cambridge Analytica, Chris Wylie, the article described how the company had gained access to the data of approximately 87 million Facebook users through a researcher at Cambridge University who had created and used

[7] This article is not the first to have reported the story, as a news article titled *The Data That Turned The World Upside Down,* published first on the Swiss website, *Das Magazin* and then in English on Motherboard by Vice, were the first to do so in early 2017. However, the *New York Times* article brought the scandal into the international limelight and started the process of governmental investigations into the data breach, as exemplified in the ETHI Committee report that identifies the New York Times article of March 2018 (ETHI Committee Final Report, 9).

a third-party application, an app, which extracted data via an Application Programming Interface (API) as part of the Facebook Platform business model (Rosenberg, Confessore, & Cadwalladr, 2018). This app innocuously invited users to take a personality quiz which, in turn, enabled the development of a program to scrape these users' profiles, and the profiles of the people on their friends list. This included demographic data, such as their location and age, as well as data about what they had liked on Facebook, what events they were interested in, or what groups and networks they were a part of (Grassegger and Krogerus, 2017). The researcher in question, Aleksandr Kogan, had "copied user data from Facebook under the guise of academic research, but had sold access to th[ose] data to Cambridge Analytica" (Vaidyanathan, 2018, p. 155). It was this latter move that violated any agreement that had governed Kogan's access to the Facebook platform for research purposes, this unsanctioned re-use of data, and it is these actions that the records refer to as a data breach.

Christopher Wylie was hired by the SCL (Strategic Communication Laboratories) Group to help found and build Cambridge Analytica. Although he left the company in 2014, Wylie was able to describe how the company used the Facebook data it had surreptitiously obtained to create targeted advertising based on the psychological profiles that SCL/Cambridge Analytica constructed (Rosenberg, Confessore, and Cadwalladr, 2018). These advertisements were used to sway voters in the 2016 US election and the 2016 Brexit vote (Rosenberg, Confessore, and Cadwalladr, 2018; Cadwalladr, 2017). Wylie explained that the goal of Cambridge Analytica was to create and use highly detailed consumer profiles to determine how to influence political behavior of potential voters, saying "they want to fight a culture war in America, (and) Cambridge Analytica

was supposed to be the arsenal of weapons to fight that culture war" (Rosenberg, Confessore, and Cadwalladr, 2018, p. 1). This was reaffirmed by Cambridge Analytica's chief executive officer, Alexander Nix, who claimed that "By having hundreds and hundreds of thousands of Americans undertake this survey (of personality traits) we were able to from a model to predict the personality of every single adult in the United States of America" (Vaidyanathan, 2018, p. 151). While it is unclear how successful Cambridge Analytica was in its goals to predict personality and use this knowledge to sway voters, the issue of their unsanctioned use of personal data remains.

In both cases, the projects that Cambridge Analytica undertook to influence voters were funded by private interests; in the United States, billionaire Robert Mercer was allegedly the main donor for the project (Rosenberg, Confessore, and Cadwalladr, 2018, p.1), while in the United Kingdom, the donor(s) have been harder to identify. Regardless, the motive to fund this work was to influence the direction and outcome of democratic elections and referenda, such as voting for a President and/or the holding of a referendum on a contentious political event (i.e., Brexit) (Cadwalladr, 2017, p.1). These activities raise fundamental concerns about accountability, informed consent, and the use of personal data scraped from commercial social media platforms for nefarious purposes.

Most suggest that this story broke in the 2018 New York Times article, while others point to a 2017 article in a Swiss publication *Das Magazin.* Yet as far back as 2015, a handful of news sources reported that a data breach had occurred. One such article from *The Guardian*, alleged that Cambridge Analytica had been accessing the personal information of Facebook users to help Ted Cruz create targeted advertisements for his campaign (Davies, 2015, p.1). At the time, Cambridge Analytica refused to

comment. For its part, Facebook stated that they were investigating these allegations and would take measures to ensure that third party companies like SCL and Cambridge Analytica did not inappropriately exploit its users' data. Facebook did not confirm nor deny the allegations (Davies, 2015, p.1). Over the next few years, similar news articles were published, yet Facebook steadfastly refused to confirm nor deny anything and largely ignored the claims (Schwartz, 2017, p.1). This did, however, change after the 2018 article in *The New York Times* made Facebook and Cambridge Analytica center stage.

Facebook routinely sells user data to data brokers and marketing companies that then create highly detailed and targeted advertisement campaigns on Facebook's platform (Vaidyanathan, 2018, p. 161). Facebook also has does business with marketing and advertising companies, offering them access to its own in-house marketing products and tools to so that they may reach and target consumers (CIPPIC, 2006, p. 19). This is part of its core business model, offering direct access to targeted audiences, although the processes of doing so are unknown and users have been generally unaware of how their data get used (CIPPIC, 2009, pp. 18-26).

The Cambridge Analytica scandal shed light on the amount of personal data that get collected, aggregated, utilized, and displayed through Facebook (Vaidyanathan, 2018, p. 161). It also highlighted the shortcomings of a business model built on maximizing the collection and use of people's data for commercial ends, which is enabled by lax internet regulation.

While the scandal may seem to some as a shocking and unusual occurrence, this Facebook/Cambridge Analytica 'data breach' and resulting use of data for advertising

and marketing is a normal business practice (Vaidyanathan, 2018, p. 159). Also, the Trump Presidential campaign and the Brexit Vote Leave campaign were by no means the first political campaigns to have employed data brokers and Facebook to reach voters for persuasive purposes, as Obama had engaged in such activities for his campaigns as well (Vaidyanathan, 2018, pp. 159-160). These were however the first campaigns to be publicly embroiled in an international scandal for doing so with big data.[8] Cambridge Analytica is not a special case, nor is it the exception to the norm when it comes to social media data profiling for marketing purposes.

This business process does, however, pose challenges to regulators, especially those concerned with privacy and personal data protection laws, which I will examine in more detail in chapter 4. The testimonies to the ETHI Committee by Christopher Wylie, representatives from Facebook and Cambridge Analytica, as well as academics and other industry professionals provide insight into the process.

1.3 The Canadian Internet Policy and Public Interest Clinic (CIPPIC) Complaint

The Canadian Internet Policy and Public Interest Clinic (CIPPIC), at the University of Ottawa, raised concerns about the ways in which Facebook was handling user data and how third-party applications had access to these data in a complaint it filed with the Office of the Privacy Commissioner (OPC) in 2009 (CIPPIC, 2009). The CIPPIC's complaint and what transpired in the Facebook/Cambridge Analytica case are similar and the issues therein were foreseen over a decade ago. The lack of regulatory

[8] Rob Kitchin notes that "there is no agreed academic or industry definition of big data" (Kitchin, 2014, p. 68), however, it is broadly accepted to be defined differently than regular data by seven characteristics: Volume, Velocity, Variety, Exhaustivity, Resolution and Indexicality, Relationality, and Flexibility (Kitchin, 2014, p. 68). The nature of big data makes it uniquely situated regarding social media and privacy, and it is a term that will be explored in more detail in the second chapter of this thesis.

action and political will since 2009 enabled the Facebook/Cambridge Analytica scandal to come to pass.

The CIPPIC complaint addressed 24 different issues about how Facebook contravened Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA). This included a concern with third-party applications, as follows:

> [that Facebook]...was allowing third-party application developers to retain a user's personal information after the user deleted the application…was allowing third-party developers access to the personal information of users when their friends of fellow network members added applications without adequate notice [to users]… was not adequately safeguarding personal information in that it [Facebook] was not monitoring the quality or legitimacy of third-party applications. (CIPPIC Complaint, 2009, p. 37)

Ultimately, the *Privacy Commissioner of Canada* found the accusation sound, noting that, "with the exception of contact information, applications technically can access virtually any personal information in a given user's account, [and that] Facebook tells users that is "does not screen or approve Platform Developers" (CIPPIC Complaint, 2009, p. 51). There were inadequate safeguards of the personal information of users, the personal information of their friends, and inadequate information available to users about how their personal data are accessed and used. Based on complaint's findings, the OPC recommended that Facebook better protect user data and privacy, such as limiting access to data by third-party applications and prohibiting third-party applications from accessing any personal information from the friends of users (CIPPIC, 2009, p. 54).

However, the OPC did not have the power to enforce these recommendations, as will be discussed later in chapter three, when addressing the details of the 2009 CIPPIC complaint with the OPC. While Facebook did implement some of the Commission's recommendations at the time, it ignored the recommendations pertaining to third-party applications and no reasoning was provided. This left the personal data and privacy of

Facebook users inadequately protected by Facebook even though some restrictions on what data third-party applications could access was implemented later on, these were not enough when it came to the protection the data of Canadian users, as the ETHI Committee later concluded. The ETHI Committee proceedings also note how the OPC lacks the authority to investigate and regulate Facebook (ETHI, 2018). Ten years after the CIPPIC complaint, some of the same weaknesses in Canada's privacy laws remain. It is unfortunate that successive governments in Canada lacked the political will to remediate this situation.

The CIPPIC complaint and the resulting report from the Privacy Commissioner of Canada will be discussed further in chapter three where I also examine the early efforts of Canadian privacy regulators and public interest groups prior to the Cambridge Analytica scandal. There I will also refer to these documents, and compare the issues they identified in 2009 with issues related to the Cambridge Analytica data breach. A key question that will be addressed is why, after nearly a decade later, so little has been done to rectify these regulatory weaknesses.

1.4 The ETHI Committee

The Cambridge Analytica and Facebook breach prompted governments around the world to scrutinize what happened. As discussed, *The Standing Committee on Access to Information, Privacy and Ethics* (2018) (the ETHI Committee) first examined how and what Canadian data were compromised. Established in 2016 to examine and discuss subjects, such as the *Personal Information Protection and Privacy Act* (PIPEDA),[9]

[9] See, for example, Evidence, Meetings 45-49, 52-55, 59-64.

Network Neutrality,[10] and the *Privacy Act*,[11] the ETHI Committee quickly focused its attention on the breach. Of the 87 million Facebook users that had their data re-used for unintended purposes, approximately 620,000 of them were Canadian. The Committee therefore assessed whether the breach had violated Canadian law.[12] The Committee also worked closely with regulators in the United Kingdom who were running parallel investigations,[13] taking a holistic and international approach (ETHI, 2018, p. 11).

The Committee spent approximately eight months examining the scandal, producing an interim report in June of 2018, and a final report in December of 2018 (ETHI, 2018). The ETHI final report was extensive with "18 public meetings to this study, during which it heard from 47 witnesses, some of them having testified more than once. It also received two briefs" (ETHI, 2018, p. 7). Witnesses included academics, regulators, and technology industry professionals. In its interim report, the ETHI Committee made 8 preliminary recommendations, and in the final report, the Committee made 26 distinct recommendations to the Canadian government on how to adapt and introduce policies and processes that would help to mitigate the risk of this kind of data breach occurring again (ETHI, 2018, pp. 25-73). Of these recommendations, 13 were to regulate social media in some capacity.

---

[10] See, for example, Evidence, Meetings 91, 92, 94, 98.
[11] See, for example, Evidence, Meetings 24-27.
[12] The Office of the Privacy Commissioner of Canada worked with the Office of the Information and Privacy Commissioner for British Columbia on joint investigations into Facebook and AIQ on the Cambridge Analytica scandal (ETHI Committee, 2018, p. 17).
[13] Predominantly the Investigation of the United Kingdom Electoral Commission (ETHI Committee Final Report, p. 11) and the Investigation of the United Kingdom Information Commissioner's Office (ETHI Committee, 2018, p. 13). Canada also had representatives (the Chair of the Canadian Committee, Bob Zimmer, as well as the Vice-Chairs, Nathaniel Erskine-Smith and Charlie Angus) on the International Grand Committee (IGC) on Big Data, Privacy and Democracy, an investigation that was led by the United Kingdom and took place over a series of meetings held by existing national-level parliamentary committees where parliamentarians from other countries were invited to participate (ETHI Committee, June 18th, 2019).

The ETHI Committee's hearings, reports, and the 13 recommendations pertaining to social media regulation to the Canadian government will be the subject of the fourth chapter of this thesis. That chapter will examine the results of those proceedings and provide a basis upon which to discuss possible paths forward for Canadian social media regulation.

1.5 Three Modes of Regulation

Academics have been examining and questioning social media regulation since social media emerged in the early 2000s (Reidenberg 2005; Benkler 2006; McChesney 2013; Winseck 2015, 2018, 2019; Wu 2003, 2010, 2018; Napoli, 2019; Gillespie 2010, 2018). The work of these scholars has explored how social media platform companies are not as well understood nor as well regulated as traditional media companies. Using the 2018 data breach as a catalyst, discussions centered around social media regulation and bringing that to the attention of governments and regulators (ETHI, 2018). What has been consistent among them is the desire to regulate social media platforms and to do so in a way that draws on one or more of the three main modes of regulation that have characterized past media sectors, such as publishing, broadcasting, and telecommunications. These three modes of media regulation are: structural, behavioral, and content regulation.

Structural regulation focuses on the physical architecture and economic power of media companies, including aspects such as their ownership, the markets they operate in and their market share with an eye to adopting legal and regulatory measures designed to ensure that no one company becomes a monopoly or accumulates too much power in either the marketplace, politics, or society in general (Wu, 2018). Behavioral regulation

focuses on the actions that a company can take about how its services are offered and how its users are treated to ensure that a company behaves ethically or in ways that are transparent to both users and to regulators (ETHI, 2018, p. 14). This includes data and privacy protection practices such as privacy policies, technical aspects such as customizable data permissions that users can control their own privacy settings and what others can see and collect about them, and requiring third-party audits (Houser and Voss, 2018, p. 37). Finally, content regulation pays particular attention to the content that is available on a company's platform, especially content that some deem harmful to users, in the hopes that by implementing practices of content moderation, social media platforms will be positive places for people to enjoy without facing harassment and hate (Keller, 2019).

In the current context, much of the discussion surrounding social media regulation has been fixated on content regulation at the expense of properly considering the potential merit of structural and behavioral regulation in the overall mediation of how social media are run. News sources regularly discuss and decry how different kinds of harmful content that platforms do not remove might negatively affects users[14] and the ways in which platforms unfairly remove other types of content that some believe should legitimately be on the platform.[15] This is due in large part because it easy to gain support

---

[14] Some examples of this are content such as blackface and other racist images or posts (*https://www.bbc.com/news/ technology-53739618),* sexism and sexual harassment (*https://www.nbcnews.com/tech/tech-news/house-democrats-facebook-do-more-about-harassment-hate-targeting-women-n1236024*), and disinformation (*https://www.theverge.com/interface/2020/7/29/21345138/facebook-viral-hydroxychloroquine-video-removal-trump-junior-stella-immanuel*).

[15] A well-known example of this sort of content removal is in the ongoing struggle of breastfeeding mothers, whose pictures of them breastfeeding on Facebook often get taken down due to Facebook identifying them as nudity. (*https://www.wired.com/2012/02/facebooks-continued-removal-of-*

because of the outcry and moral panic around either sensationalist content and cases of extremely negative content such as cyber-bullying, revenge porn, or terrorist rhetoric (Gillespie, 2018, pp. 8-9). Also, content by way of text posts, pictures, and videos are the most visible aspect of social media. In addition, people using social media can readily express their opinions about what they see on social media. The Cambridge Analytica scandal shifted the narrative on social media regulation and put a spotlight on privacy and data protection instead. Governments began to consider structural and behavioral questions related to the design of the platform, business models, and ownership, among other aspects, aiming to determining how social media affect society more broadly.

The mode(s) in which a government decides to regulate any sort of media, whether that be news press, publishing, broadcasting, telecommunications, or social media, is based on a number of factors, including how media are defined by the government, how the government defines and addresses privacy and data protection, whether or not the internet is understood as the free-wheeling terrain of diversity, competition and choice or one that is increasingly being consolidated into the hands of a relatively small number of internet behemoths such as Google, Apple, Facebook, and Amazon (the so-called GAFA group of internet giants). In the thesis I will define what a social media platform is and discus the different modes of regulation raised by the Cambridge Analytica scandal. There I will also review the literature about media

---

breastfeeding-pictures/. https://www.washingtonpost.com/news/the-intersect/wp/2015/02/26/facebook-is-embroiled-in-yet-another-breastfeeding-photo-controversy/. https://www.dailymail.co.uk/femail/article-4650418/Facebook-user-ordered-remove-photo-breastfeeding-mum.html).

regulation, to see the direction social media regulation has been going in the past several years and how that is related to the Cambridge Analytica data breach.

1.6 A Note on Methodology

The methodology that I employ in this thesis is that of textual analysis and discourse analysis. I will first be examining selected literature on topics relating to media regulation and social media in regard to the three main modes of regulation. I will then be analyzing the final report that came out of the 2009 CIPPIC complaint with the OPC, closely reading and discussing the recommendations presented therein. I will then turn my attention to key proceeding documents from the ETHI Committee inquiry hearings, as well as the interim and final reports generated from the inquiry to identify the most important elements of the inquiry, as well as to analyze and explore the recommendations that the Committee put forward. Throughout this process, I will be drawing on key regulatory and legislative documents, such as the *Personal Information Protection and Electronic Documents Act (*PIPEDA) and the *General Data Protection Regulation* (GDPR).

1.7 The Future of Facebook Regulation in Canada

This thesis therefore seeks to explore the question of social media regulation in Canada through the lens of the Cambridge Analytica and Facebook data breach scandal. It will be informed by the ETHI Committee, seeking to clarify where the Committee's recommendations related to social media regulation and identifying shortfalls in terms of preventing another Cambridge Analytica like scandal. The thesis will also consider the three different modes of regulation; structural, behavioral, and content regulation; to identify what the best approach to social media regulation in Canada and other countries

might be. The thesis concludes by suggesting that protecting privacy and personal data on social media platforms — a behavioral model of regulation with some potential elements of structural regulation — might be the best approach to ensure that social media users in Canada are protected and that social media operate in the public interest[16] and in a democratic way.

[16] The government of Ontario explains that "the concept of 'public interest' is not easy to define, and it varies in different contexts. In a regulatory setting it speaks to the importance of transparent, inclusive, and rigorous processes with clearly understandable and impartial decision-making frameworks. As Pal and Maxwell suggest, the public interest also involves, taking a balanced approach to regulatory outcomes in terms of the various interests involved, but also in terms of equilibrium among individual consumer and citizen interests, commercial interests, and broad Canadian societal values (Pal and Maxwell, 2004). In legal terms, the University of Toronto Faculty of Law defines public interest as a "broad umbrella that describes legal work that shares a common feature: furthering interests shared by the public (or a significant group therein) or addressing public concerns. Its scope is so wide that it may include discrimination and equality issues, environmental protection concerns, constitutional rights, special interest clients such as women, children, refugees and immigrants, work for charities and non-profits, legal aid work and more" (University of Toronto, 2021 p.1).

Chapter 2: Facebook Unchecked? Modes of Media Regulation

2.1 Literature Review

There have been three dominant approaches to communications and media regulation: structural, behavioral, and content focused. Over the course of the 20th Century, different combinations of these broad approaches have formed the basis of three distinct forms of communication and media regulation: telecommunications, broadcasting, and publishing (Babe, 1990, p. 17).

Today, the rise of a new class of internet companies, like social media platforms, has challenged these traditional distinctions and raised questions about which, if any, of these three modes can best be applied to internet companies such as Facebook, Google, Twitter, Amazon, and Reddit, just to name a few. This becomes more difficult since each of these companies is engaged in a range of different communication and media

activities, meaning that there is no "one size fits all" type of remediation when it comes to social media. This chapter begins with a review of some of the literature about current approaches to regulation and discusses different approaches adopted to regulate telecoms, broadcasting and publishing sectors in the United States and Canada. This is followed by a review of a body of literature that questions the adequacy of these in the current context and if they can be useful to inform a new generation of internet regulation in Canada. These will be examined in reference to the Cambridge Analytica scandal, and what modes of regulation might mitigate risks to privacy and personal data protection. This section will situate Facebook as it stands now in terms of regulation in Canada and will provide a brief review of the history of how media have been regulated in Canada. The history of publishing, broadcasting, and telecommunications media regulation in Canada is different from that of the United States, despite being inextricably linked by proximity, technology, politics, and media ownership. Robert Babe (1990), a Canadian communication scholar, in his work on the history of the communications industries in Canada, noted that "it is particularly important to recognize the constants or patterns in the historical development of Canadian telecommunications… Much of the current thinking of our all-too-often ahistorical minded policy-makers are shrouded in misconception, even myth" (Babe, 1990, p. 4). Thus, here I chose to situate the Cambridge Analytical scandal as a historically important catalyst, to assess the role that both corporate and governmental interests play in shaping infrastructure, processes, and implementation of media technologies (Babe, 1990, p. 4). Babe's work provides a framework with which to understand how Facebook regulation in Canada came to be.

More specifically, Babe provides insight into how the three main sectors of the Canadian communications industry – publishing, broadcasting, and telecommunications – have been regulated since their inception. Traditionally, publishing was regulated through copyright, slander, and libel laws, with very little in terms of the regulation of the content publishing companies can and cannot publish. In contrast, broadcasting has been extensively regulated under the *Broadcasting Act* (1991) and the *Radiocommunications Act* (1985). Indeed, under both acts, the government plays a strong role in determining who does and does not get a broadcasting license. This strong lever to some extent determines the structure of the broadcasting industry in terms of who can and cannot (e.g. non-Canadians) enter the broadcasting business while also shaping the behaviour of broadcasters in several ways. For example by making access to a broadcasting license conditional upon, most notably, commitments to creating and distributing minimum levels of Canadian content, that is "content that meets the needs and interests of Canadians" and by putting broadcasters under the regulatory authority of the Canadian Radio-television and Telecommunications Commission (CRTC) (CRTC, 2020). According to the CRTC,

> broadcasting plays a critical role in helping build and support our Canadian identity. In recognition of this, Canada's Broadcasting Act sets out objectives to ensure that Canadian broadcasting content meets the needs and interests of Canadians. The CRTC then sets policies and rules to ensure that those objectives are put into practice in Canada's broadcasting system (2020).

In short, broadcasting regulation means that the government directly affects the structure, behaviour, and content of the industry by imposing obligations through the licensing process. This role for government to shape the structure, behaviour, and content of broadcasting, when compared to the ideals of a free press and free speech;

seem at odds but is justifiable when considering the allocation of limited broadcasting resources such as radio spectrum; and in an environment that leans toward a concentrated ownership. In this regard, this strong regulatory regime distinguishes the publishing, broadcasting, and telecommunications.

Telecommunications regulation has been more structural and behavioural. The concerns of telecommunications regulation are market dominance, common carriage, technical standards, pricing, and social goods such as affordable universal service (Babe, 1990, p. 17). These have been persistent features of telecommunications regulation since the early 20th Century as seen in the current *Telecommunications Act of 1993*[17] with its seven core objectives to ensure that telecommunications platforms maintain Canada's identity and sovereignty and the concept of common carriage, which, broadly speaking and in sharp contrast to broadcasting and publishing, prevents telecom operators from controlling or influencing the content they carry.

Some aspects of social media companies fall within traditional media regulation, and some aspects are outside of traditional regulatory silos. This is because social media companies are hybrid companies which I will describe in more detail later. Because there

---

[17] Which was first passed in 1993, three years after Babe's book. As Innovation, Science and Economic Development Canada (ISED) explains, "Until the *Telecommunications Act* was passed in 1993, telecommunications carriers were regulated under several different Acts, including the Railway Act and the other Acts... To complicate matters, some telephone companies that carried on business in only one province were regulated by provincial public utilities commissions rather than the CRTC, and others were subject to company-specific legislation, such as the *Bell Canada Act*. https://www.ic.gc.ca/eic/site/110.nsf/eng/00006.html

is no single Act or legislation that has been developed solely for social media entities, they can and do fall under the purview of other regulation and legislation. Current proposals from the Broadcasting and Telecommunications Legislative Review (BTLR) Panel (2020), for example, would bring *some* activities of social media companies, such as Facebook's WhatsApp or Apple's FaceTime, under a revised *Telecommunications Act* (Recommendation 16). At present, the business models and activities of social media companies related to data protection and privacy are already covered by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and fall under the authority of the Office of the Privacy Commissioner (OPC) as will be seen in chapter three. When it comes to copyright issues concerning content, social media are subject to the *Copyright Act* and, therefore, the purview of the Canadian Intellectual Property Office (CIPO). While the BTLR report does offer some modest recommendations with respect to structural regulation and better privacy and data protection, its main concern is the reshaping of 20th Century broadcasting content regulation to 21st Century internet-based media.

The structural mode of regulation, for example, focuses on addressing issues regarding the ownership and structure of communication and media markets. For example, a key issue for structural regulation is media ownership concentration. Thus, structural regulation puts limits on how much of a media market a single company can own. In so doing, structural regulation aims to curb the influence and power that comes with monopolies or oligopolies, wherein companies can effectively set, for example, price levels, service availability, and personal data protection and for regulatory oversight to set minimum standards for each. This would be the case where one or two companies

corner the market on a particular service providing them with the power to make choices that do not benefit consumers since there are no competitors.

Robert McChesney (2013), addresses such questions in relation to the telecommunications sector in the US, explaining that,

> the consequences of the monopoly system are evident. In 2000, the United States was a world leader in terms of broadband penetration and access, "12 -24 months ahead of any European country," according to the Danish National IT and Telecom Agency (p. 114). Today, the United States ranks between fifteenth and thirteenth in most global measures of broadband access, quality of service, and cost per megabit. In a September 2011 global report from Pando Networks, the United States ranked twenty-sixth in the world for average consumer download speed. A 2012 New America Foundation examination of twenty-two cities worldwide concluded that "US consumers in major cities tend to pay higher prices for slower speeds compared to consumers abroad." "Here's a big fact," the author of the FCC's National Broadband Plan, Blair Levin, stated in 2012; "For the first time since the beginning of the commercial Internet, the United States does not have a commercial wireline provider with plans to build a better network than the currently best available network." Crawford, [an advisor to the Obama Administration] notes that this means most Americans will never get access to "the speeds the rest of the world is used to." (McChesney, 2013, p. 114).

In other words, McChesney suggests that concentrated telecoms and broadband internet markets are bad for Americans and bad for America.

Another important proponent for the structural approach to communications regulation is Tim Wu. Wu became famous for coining the term "network neutrality"[18] back in 2003, a concept based on common carriage principles that are hundreds of years old that combines both structural and behavioural modes of regulation. This does so by

[18] Network Neutrality in Canada is defined by the Canadian Radio-Television and Telecommunications Commission (CRTC) as "the concept that all traffic on the Internet should be given equal treatment by Internet providers with little to no manipulation, interference, prioritization, discrimination or preference given" https://crtc.gc.ca/eng /internet/diff.htm. On the other hand, while Network Neutrality existed in the US up until 2017, it has since been removed by the Trump administration, and repeals against this move have not been successful, https://www.reuters.com/article/us-usa-internet-idUSKBN20032K

separating a company's control over distribution networks from the content carried over those networks while also ensuring that network access providers cannot discriminate against services and content (Wu, 2003).

Wu is also an established expert of antitrust regulations in the United States (Wu, 2010, 2016, 2018). His book, *The Curse of Bigness, Antitrust in the New Gilded Age* (2018), examines how the United States dealt with regulating large corporations. As Wu observes, many of the issues that regulators faced in the late 1800s to the early 1900s remain in this age of internet giants like Facebook, Google, and Amazon. Older cartels, such as Standard Oil under John D. Rockefeller, John Pierpont Morgan's US Steel and railroad monopolies, and the telecommunications giant, AT&T, were largely ignored by government, enabling them to construct monopolies in the industries they dominated, paying workers low wages with few services offered for consumers to chose from (Wu, 2018). It was only in 1902 that President Theodore Roosevelt began to fight against the trusts, using the *Sherman Act*, legislation first enacted in 1890 which effectively banned monopolies by decreeing that "every person who shall monopolize, or attempt to monopolize… any part of the trade or commerce among several States, or with foreign nations, shall be deemed guilty of a felony" (Sherman Act, section 2 in Wu, 2018, p. 31).

The wording of the *Sherman Act* is both broad and harsh in tone, as it was meant to be widely applicable to corporations that threatened the democratic process through their sheer size and power. Even though Roosevelt maintained a healthy admiration for big business, he nonetheless recognized that they should not be allowed to consider themselves above the law (Wu, 2018, p. 49). Siva Vaidyanathan (2011; 2012) who has studied and written about Google and Facebook for a decade, raised similar concerns

about the corporate degradation of democracy but focused specifically on the search engine and social media giants. In particular, he sees Facebook's role as being fundamentally at odds with democracy, pointing to how Facebook undermines public deliberation on important social issues by promoting sensationalist content over journalistic integrity, fragments people's attention via constantly changing and distracting content that demands we split our focus, and how its platform can be used to spread misinformation through fake news, and targets those who voice opinions that go against the systems in power as seen in Saudi Arabia with the way that the government uses social media to track down dissenters (Vaidyanathan, 2018).

Because of this continued concern of monopolistic firms threatening democracy through their sheer size and reach, Wu's position on social media giants is that governments need to return to antitrust laws to ensure that no social media platform becomes more of a monopoly than it already is (Wu, 2018). In the United States specifically, antitrust laws make it possible to prevent one company from being involved in too many different types of services or markets (Wu, 2018, p. 31). According to Wu, social media platforms and internet giants in general; Facebook, Google, and Amazon specifically; have been a blind spot for anti-trust regulators. He describes Facebook's rise to power, noting that in its early days, Facebook quickly overpowered MySpace, its only competitor at the time (Wu, 2018). Then, in 2010, when Instagram became popular, positioning itself as a rival to Facebook with is social media photo service, Facebook bought the competition with nary a concern raised by US and U K competition authorities. According to Wu the U. K.'s 'do-nothing' rationale was as follows:

> Facebook did not have an important photo-taking app, meaning that Facebook was not competing with Instagram for consumers. Instagram did not have advertising revenue, so it did not compete with Facebook either. Hence the report was able to reach the extraordinary conclusion that Facebook, and Instagram were not competitors (Wu, 2018, p. 123).

In 2014, Facebook then bought WhatsApp, a secure messaging service that rivaled Facebook's messenger function. By buying out the competition, Facebook was cornering the market on social media services, something that was overlooked by US anti-trust law makers but was no different than the historical precedents against the oil, railroad, and telecommunications trusts over the last century (Wu, 2018, p 51). Today, anti-trust regulation in the US is but a shadow of its former self, as seen by how social media platforms have been exempt from anti-trust actions, and Facebook is a perfect example of that.

Adopting an antitrust approach to social media regulation as Wu suggests could help ensure, at a structural level, Facebook could not monopolize the social media market leaving users no other option, such as is the case with WeChat in China. If Facebook is allowed to dominate social media platform services, it can decide what aspects or services it deems most important and may very well neglect other services that users want, not unlike the situation with the Canadian companies mentioned above. Also, if its monopoly power remains unchecked — it will have the ability to unilaterally set terms and conditions for the price and use of its services as there will be no other competition, and Facebook's control over large swaths of the market will allow it to wield power over

advertising and direct user traffic within their own services and externally to partners.[19] This creates a walled garden situation, where users find themselves staying within the confines of one social media ecosystem. Furthermore, Facebook can set the standard on data protection and privacy from an industry perspective[20], which they can weaken to serve their business model of reselling personal data to third parties for advertising to target specific demographics (Srinivasan, 2019).

In *The Curse of Bigness* (2018), Wu provides ways in which structural regulation and antitrust laws can make a come back to mitigate this social media platform concentration. Wu suggests reviewing mergers and acquisitions in this sector, noting that anti-trust laws were meant to erect meaningful barriers against one company taking over too many other would-be rivals in the same field (Wu, 2018, p. 128). In Facebook's case, this would have meant mitigating the merger with Instagram. Wu also suggests making merger processes more open to public scrutiny would help to ensure that anti-competitive mergers be stopped (Wu, 2018, p. 129). Wu also looks to European anti-trust processes and argues that US regulatory bodies could benefit from following their example. As while strong anti-trust measures in the US dropped off, regulators in the European Union (EU) still bring cases against monopolistic companies, to hold them accountable for anti-

---

[19] Facebook's worldwide revenue in 2018 was $55.1 billion, ten times what it had been just six years earlier. Facebook proper has 2.3 monthly users, 1.6 billion people use its WhatsApp social messaging service, a billion people use Instagram and 1.3 billion use Messenger monthly. While the average social media user in the US uses seven social media type services, Facebook accounts for over half of that use, with the average American spending close to an hour a day — or a fifth — of their time online on Facebook (or Instagram). Worldwide, it accounts for over two-thirds of social media use, leading to the perception in some parts of Southeast Asia — where it is often bundled into mobile phone plans that do not count its use towards people's data allowance — that Facebook is "the Internet" (Facebook 2019: 37-38, cited in Winseck, 2020, p. 4).

[20] Regulatory standards exist, such as the EU's GDPR, but from an industry perspective, internet giants can set the "expected standards" for a particular industry, as smaller companies look to them for an example of how to run their companies.

competitive behaviours through the development of structural and behavioural regulations. Wu observed that "European antitrust is far from perfect, but their leadership and willingness to bring big cases when competition is clearly under threat should serve as a model for American enforcers and the rest of the world" (Wu, 2018, p. 131).

In addition to the EU as a model, Wu also explained that regulators today — like their predecessors in the early 20th Century — should consider breaking up internet giants that prove to be too big to effectively regulate. Yet, he adds, too often this option seems to be seen as being beyond the pale, yet the threat of break-ups is currently the best remedy against companies like Facebook, who have already grown too big to effectively regulate. He suggests, for example, that regulators "consider a breakup of Facebook [to undo] the mergers with Instagram and WhatsApp. While Facebook might not like being dissolved, and might find the competition unwelcome, it is hard to see what the great social cost, if any, would be" (Wu, 2018, pp. 132-133). If Facebook, Instagram, and WhatsApp were competitors, it would become far easier to boycott a service that did not have good privacy and data protections for users because they could choose to opt-out of Facebook, but still be active and connect to friends on Instagram if they were happier with Instagram's policy on privacy, thus providing consumer choice. Furthermore, to retain users, different social media services would have to compete to offer an ideal experience to users, considering public want and need when it comes to issues of privacy and data protection. Add that to the already stated issues of market dominance identified by Vaidyanathan (2018), such as political influence and undermining democracy, and it becomes clear that breaking up and preventing the creation of large monopolies such as

Facebook should be a first line of structural regulation, rather than as a last resort approach.

Canada, like the US, has had legislation to prevent media market concentration for decades but it has been weak and ineffectual. For example, in the field of broadcasting and telecommunications, "Canada differs fundamentally from its international peers in terms of its extraordinarily high levels of diagonal and vertical integration across the network media economy" (Winseck, 2018, p. 42). This is due in part to the fact that Canadian regulators are hesitant to regulate broadcasting and telecommunications more rigorously as this might discourage these industries from supporting Canadian culture and values. As Winseck observed, it is common that "questions about media ownership and the structure of media markets are "off-limits" in the mainstream discourse" (Winseck, 2018, p. 44). The result of higher levels of concentration is that companies like Bell Canada, who own both telecommunications and broadcasting, can choose to focus revenue on the telecommunications side rather than the broadcasting side (Winseck, 2018, p. 43). The result, according to Winseck, is that broadcasting continues to be underfunded in Canada while Canadians pay more for basic internet access and telecommunications services. Because of this historical tendency to shy away from stricter regulation, Canada is not able to fall back on pre-existing regulatory frameworks as the US can.

While the structural mode of regulation might not be an approach that Canada could enforce since Facebook head quarters is in the US, a discussion between countries around structural modes of regulation is an option. Germany, for example, applied a form of structural regulation to control Facebook's ability to share people's data across its

three services: Facebook, Instagram, and WhatsApp.[21] These measures have effectively stopped Facebook from collecting and aggregating German users' data from all three services from one platform. Canada could follow a similar path.

While structural regulation focuses on the ownership aspect of regulation, the behavioural mode of social media regulation focuses on actions that companies can take to ensure specific outcomes in their service offers, rather than limiting how many services or infrastructure a company can own. One of the clearest examples of this approach is the European Union's *General Data Protection Regulation* (GDPR), which came into full effect on May 25th, 2018. The GDPR requires that a company ensure that its users' data and privacy are protected against exploitation and unnecessary exposure to third parties through processes like third-party verification, and through monitored and enforced Terms of Services. The GDPR also requires EU member states to establish designated privacy authorities (DPAs) with the power to investigate companies who may not be protecting their users' data and privacy in line with the GDPR standards and the ability to enforce fines and penalties on companies that are found to contravene the GDPR (Denham, ETHI, 2018, 106, p. 2).

Kimberly A. Houser and W. Gregory Voss (2018) explore "the differences between American and European privacy standards and what the GDPR will mean for US companies, using Google and Facebook cases as examples" (p. 6). They describe how the GDPR by enforcing behavioural regulations that apply to Facebook and Google outside of the EU and, in so doing, reveal the failures of US privacy laws. They start by

---

[21] The case summery of Germany's Federal Cartel Office decision can be found here; https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568

explaining how in the EU, personal data protection and individual rights to privacy are based on the Organisation for Economic Co-operation and Development's (OECD) recommendations derived from the core principles of fundamental human rights involving personal data ownership and the right to be forgotten (Houser and Voss, 2018, pp. 7-8). The GDPR, and before it, the European Data Protection Directive 95/46/EC[22], are meant to harmonize privacy regulation across the EU, providing a framework for DPAs. Unlike the EU, the US does not have a harmonized, federal privacy law and data protection is provided based on sectors (Houser and Voss, 2018, p. 10). As a result, data protection and privacy law in the US is fragmented under several different Acts depending on the sector it is under[23], making it harder for regulation to be implemented across the country. As a result, there is no overarching guiding set of principles in the US for privacy and data protection. In Canada, PIPEDA does provide some guidance, as will be discussed later.

The main regulatory body for issues related to privacy breaches is the Federal Trade Commission (FTC). Yet, according to Houser and Voss,

> there is no federal legal requirement in the U.S. for internet service providers to maintain privacy policies informing users of how their information will be used, nor are companies required to obtain permission

[22] The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals about the processing of personal data and on the free movement of such data is the predecessor to the GDPR and was based upon the same notion of privacy and data protection being a fundamental human right (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046).
[23] Some categories of data protection and privacy covered under federal law are healthcare data (under the Health Information and Portability Accountability Act, HIPAA), financial data (under the Gramm Leach Bliley Act, GLB), children's information (under the Children's Online Privacy Protection Act, COPPA), students' personal information (under Family Educational Rights and Privacy Act, FERPA), and consumer information (under the Fair Credit Reporting Act, FCRA), but, significantly, these statutes were enacted prior to significant personal use of the internet (Houser and Voss, 2018, pp. 10).

> to use the data, companies that do supply privacy policies can be subject to action for failing to comply with them (2018, p. 10).[24]

The FTC's inability to hold companies' accountable means that even when cases of data protection and privacy are brought against social media platforms, they seldom result in any sort of meaningful enforcement.

The introduction of the GDPR granted greater powers to EU members to pursue enforcement actions against US companies that do not comply with EU regulation, making up for the lack of regulation in the US. These greater powers include the ability to perform third-party audits of any company suspected of violating EU privacy laws and the ability to fine these companies with sums that will make them take regulation violations seriously.[25] What this means for US companies, including social media platforms, is that they will have to be much more careful when dealing with data from EU members, especially because of the exterritorial reach of the GDPR. As Houser and Voss (2018) and other authors such as Miglicco (2018) emphasize, the GDPR applies to "all organizations handling the personal data of EU citizens or residents" (Miglicco, 2018, p. 10) regardless of where these organizations are geographically located. This means that "when you are moving data from company to company, or country to country, the rules applying to that data move with it … [therefore] cloud providers hosting GDPR protected data are impacted by the law" (Miglicco, 2018, p. 11).

---

[24] Arguably, this facet of US law actively encourages social media platforms not to invest time an energy into maintaining proper privacy policies, lest they be subject to upholding them.

[25] While there have been hundreds of enforcement actions taken against US tech companies in recent years, 163 the low maximum fines permitted under the laws created pursuant to the 95 Directive have not been substantial enough to force change in the way these technology companies collect and utilize data. This will change with the extraterritorial jurisdiction and enormous fines possible under the GDPR (Houser and Voss, 2019, p. 36).

The location where data are stored was also raised during at the ETHI Committee meetings, when Kevin Chan, CEO of Facebook Canada commented that,

> I want to be clear. Prior to today, prior to our data policy changes, Canadians were served by Facebook Inc. in California, and the entity with which they contract was Facebook Inc. That remains the same, so there's no change with regard to Canadians (ETHI, 2018).

Therefore, according to Chan, since Canadian data are physically stored in the US, the protection of the personal data and privacy of the data of Canadians is governed by the weak US standards rather than Canada's. This is what occurred to Canadian users affected by the Cambridge Analytica scandal, whereby their data ought to have been protected against third-party reuse under PIPEDA, as stated in the 2009 Complaint against Facebook by the CIPPIC. However, because Facebook servers were in the US, and the Office of the Privacy Commissioner of Canada does not have any real enforcement powers, Facebook did not take steps to protect Canadian data as per the OPC request in response to CIPPIC's 2009 complaint (OPC (2009), ETHI (2018)). Had those measures been in place, Cambridge Analytica would not have been able to obtain the data of Canadians in the first place.

The Broadcasting and Telecommunications Legislative Review (BTLR) – a process aimed at modernizing the legislation governing Canada's communications sector and that began in 2018, and concluded in 2020 with a Final Report released in January – made some suggestions that echoed the requirement for extraterritorial jurisdiction over data and data practices. The final report *Canada's Communications Future: Time to Act* stated that, "Canada's privacy regime is no longer suited to the present-day environment and does not adequately address the potential risks posed by communications technologies" (BTLR, 2020, p. 186), identifying how:

> The European Union's *General Data Protection Regulation* (GDPR) has in effect become a global standard with respect to the privacy of individual data. The GDPR regulates the processing by an individual, a company, or an organization of personal data relating to individuals in the EU. It harmonizes national data privacy laws and does not permit data to be transferred to a non- EU country unless that jurisdiction has an adequate level of data protection…Given the importance of personal information in how communications services operate, Canadian communications statutes should contain a broad, unified, cross-sector policy commitment to privacy and confidentiality of communications services, over and above the provisions of PIPEDA as the law of general application. Canada should also take steps to address adequacy with respect to global privacy standards (BTLR, 2020, pp. 186-187).

While the BTLR approach offers modest recommendations in line with structural and behavioural regulatory approaches, its emphasis is overwhelmingly on content regulation and, more specifically, on updating the long-standing history of broadcasting regulation in Canada. It zeros in on using content regulation to protect and assert national sovereignty through managing Canadian content regulation[26] in the context of a more internet-centric communications and media system, such as through streaming services that circumvent the more traditional broadcasting methods of delivering content to audiences. During the BTLR panel's efforts, it was suggested that social media could be better regulated under a revised version of the *Broadcasting Act*. Specifically, the report states that all:

> those providing media content services to Canadians – whether online or through conventional means, whether foreign or domestic, whether or not they have a place of business in Canada – [should be brought] within the scope of the Broadcasting Act and under the jurisdiction of the CRTC (BTLR, 2020, p. 11).

---

[26] One of the main goals of Canadian Content regulation (CANCON) "is to ensure that Canadian broadcasting content meets the needs and interests of Canadians by delivering **compelling, high-quality Canadian-made creative content** from diverse sources on a variety of platforms (https://crtc.gc.ca/eng/cancon.htm).

In addition, to reflect this much broader mandate for the CRTC, the BTLR recommended that it should be renamed as the Canadian Communications Commission (CCC). The BTLR report also calls for a new *Media Communications Act* to replace the *Broadcasting Act*, reflecting the much broader scope for the new act.

The upshot of this proposal is that distinctions between traditional broadcasting and internet companies would be superseded by, as the report recommends, the term 'media content undertaking' to replace the 'broadcasting undertaking' in the Act and to instead cover three types of media content undertakings such as 1. media curation undertakings, 2. media aggregation undertakings, and 3. media sharing undertakings (BTLR, 2020, p. 31). The latter two categories would capture social media, with the result that companies such as Facebook, Google, Twitter, and so forth would become extensively and formally regulated by the renamed CCC. In this regard, the BTLR puts forward some interesting ideas to consider in terms of social media regulation. Even so, because of the content focused nature of the proceedings and the resulting recommendations, I will not focus on the BLTR as it is beyond scope. Regardless, the call for Canadian legislation to better align with the GDPR has come from multiple actors, beyond the ETHI Committee investigation into the Cambridge Analytica scandal.

2.2 Data Brokers and Big Data

There is also another important set of actors, data brokers and big data companies. Data brokers collect, aggregate, and exchange personal data to be reused and exploited in the way Cambridge Analytica did. Data brokers as defined by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) are companies "whose primary business involves the trading and analysis of personal information" (CIPPIC, 2006, p. 4). The US

Federal Trade Commission (FTC) is more expansive in its definition, for them data brokers are:

> companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud (FTC, 2014, p. 3).

While CIPPIC's definition is shorter than the FTC's, both are broad enough to suggest that Facebook is also a data broker, but there are some distinctions. Although social media make up a significant portion of the data ecosystem by sheer data volume alone, social media platforms also have access to very rich user data profiles, and offer advertising services to marketing companies, they generally do so by relying "on commercial data brokers to supplement their own user data with "offline data" about users' lives away from their sites" (CIPPIC, 2018, p. 4).

In most cases, Facebook collaborates with data brokers to offer marketers data-based advertising services that benefit both the marketers and Facebook. As the CIPPIC discovered services like Facebook's "onboarding tool known as 'Custom Audiences'" allows marketers to use offline data combined with Facebook's user data to create detailed marketing profiles, while their "Lookalike Audiences allow marketers to expand their advertising reach through segments of Facebook users that resemble a specified group" (CIPPIC, 2018, p. 19). Facebook is also in the business of directly selling its data troves to data brokers, who then market those data, often in combination with other data sources, to advertising and marketing companies.

What sets Facebook apart from being purely a data brokerage company, however, is how it collects the data that it uses and the fact that it provides services to users that are publicly available. This public-facing aspect of social media platforms makes them more

apparent and therefore makes them more likely to come under scrutiny by regulators for their business practices when it comes to the collection and use of personal data. At the same time, however, this facet of social media allows for Facebook to describe itself not as a data brokerage company, but as a technology company (Napoli, 2019, p. 7). Specifically, Facebook positions itself as a service provider, like an internet service provider (ISP), allowing access to content rather than as a company that deals in personal data – a rather disingenuous claim since ISPs provide access to the internet, while Facebook restricts access to its own platform and services. The ways in which Facebook chooses to define and present itself has had, and continues to have, significant implications for how a government can regulate the company.

While business as usual may see personal data routinely be transferred between Facebook and data brokers, the reason the Cambridge Analytica case is different is that although Cambridge Analytica is essentially by definition a data broker[27], they did not partner with nor use their own API to the Facebook platform when they used Facebook's user data. Instead, they partnered with an individual acting as a third-party application on Facebook's platform to obtain the data for them. This was the differentiating characteristic between how Facebook enters into contractual agreements with data brokers, and the unsanctioned use of data by Cambridge Analytica. The term "unsanctioned" is the term used in this thesis to refer to how Cambridge Analytica reused Facebook data – as the way the data were obtained by the first company was according to

[27] Cambridge Analytica's parent company, the SCL Group identifies its role through a slogan that reads "The population is the prize, elections are the battleground" to explain the different data driven solutions it has to offer to election campaigns and marketers based on data profiles and demographic mapping. https://sclgroup.online/.

the usual third-party agreements that Facebook has, but they were then collected and were reused by Cambridge Analytica in ways that were not sanctioned by Facebook. Facebook actively encourages third-party applications to purchase access to data from the platform, this is legal and sanctioned by the company, but those agreements do not include the reuse of those data for purposes they were not intended for in agreements. Cambridge Analytica's use of the third-party data collected by Aleksandr Kogan, was not sanctioned.

Siva Vaidyanathan clarifies the distinction between unsanctioned Facebook data reuse and the regular practices that Facebook engages in:

> Until 2015 it was Facebook policy and practice to let application developers tap into sensitive user data as long as users consented to let those applications use their data. Facebook users were never clearly informed that their Friends' data might also flow out of Facebook or that subsequent parties, like Cambridge Analytica, might reasonably get hold of the data and use it however they wished. (Vaidyanathan, 2018, p. 160).

The 2009 CIPPIC complaint against Facebook with the Office of the Privacy Commissioner of Canada (OPC), focussed on the fact that Facebook did not verify or audit the third-party applications that use its platform is the main reason that Cambridge Analytica was able to obtain and use the data in a way that was legal, but unsanctioned, and not technically a data breach.

As it stands, data brokers like Cambridge Analytica are largely understudied and unregulated, especially in the US. While Canada has the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) that applies broadly to all companies that collect and use personal data and which fall under federal jurisdiction, the US does not have a comprehensive framework to protect personal privacy and data, either online or off. The CIPPIC explains that,

> PIPEDA requires organizations to obtain the informed consent of individuals for the collection, use and disclosure of their personal information. Those purposes must be ones that a reasonable person would consider appropriate in the circumstances. And organizations must adopt safeguards appropriate to the sensitivity of the information held (CIPPIC, 2006, p. 35).

This requirement, however, does not automatically mean that data brokers in Canada are comprehensively regulated. In undertaking the investigation for their report, the CIPPIC (2006) noted that common "data broker practices pose compliance challenges to each of these elements of PIPEDA" (p. 35) since PIPEDA does not have strong enforcement measures. This creates a situation where data brokers operate from the margins, without the same scrutiny that traditional media companies get; yet they wield immense persuasive power, and have access to significant amounts of personal information. While it is outside of the scope of this thesis, as a comprehensive study of the relationships between data brokers and Facebook would be necessary to fully understand and address the issues of privacy and personal data protection on social media platforms.

Big data, on the other hand, is somewhat of a buzzword:

> commonly used in business circles and the popular media, with regular commentaries in, for example, the *New York Times* and *Financial Times*, and feature pieces and sections in popular and science magazines such as *The Economist*, *Time*, *Nature*, and *Science*" (Kitchin, 2014, p. 67).

Even though there is no single agreed upon definition of big data Rob Kitchin has identified seven common characteristics that set big data aside from other kinds of data (Kitchin, 2014, p. 68). These seven characteristics are: volume, velocity, variety, exhaustivity, resolution and indexicality, relationality, and flexibility explained as follows:

- Huge in *volume*, consisting of terabytes or petabytes of data;
- High in *velocity*, being created in or near real-time;
- Diverse in *variety* in type, being structured and unstructured in nature, and often temporally and spatially referenced;
- *Exhaustive* in scope, striving to capture entire populations or systems (n= all), or at least much larger sample sizes than would be employed in traditional, small data studies;
- Fine-grained in *resolution*, aiming to be as detailed as possible, and uniquely *indexical* in identification;
- *Relational* in nature, containing common fields that enable the conjoining of different datasets;
- *Flexible*, holding the traits of extensionality (can add fields easily) and *scalable* (can expand size rapidly) (Kitchin, 2014, p. 68).

It is these characteristics, that make big data more useful to advertisers and marketers since capturing highly detailed information about entire populations in real-time allows for advertisements to be tailored and targeted to consumers in a comprehensive way. Big data by their nature in a social media context also inherently pose more risks to privacy than small data since individuals are highly identifiable and targetable. Big data therefore appeal to marketers and are a challenge for regulators. It is much easier to secure the informed consent of individuals to use their data through mechanisms such as surveys and focus groups traditionally employed by small data projects, which includes census taking, whereas the blanket consent that is asked of social media users when they first sign up for a social media service is most often agreed to by uniformed users, making 'real' consent questionable. As Obar and Oeldorf-Hirsh (2018) state, consent on social media platforms has been called "the biggest lie on the Internet, which anecdotally, is known as 'I agree to these terms and conditions'" (p.1). In their recent study of privacy policies online their "qualitative findings suggest that participants view policies as

nuisance, ignoring them to pursue the ends of digital production, without being inhibited by the means" (Obar and Oeldorf-Hirsh, 2018, p.1).

The reason that big data as a term is important to understand in the context of Facebook, and social media in general, is that these platforms all deal in big data. The data that Facebook collects and sells about its users is extremely high in volume, is created in real-time as users interact with the platform, is varied in type based on multiple data points for each action a user takes on the platform include multiple media, and is exhaustive in terms of scope considering that there are approximately 2.50 billion monthly active users (MAUs) on Facebook as of December 31, 2019 (Facebook, 2019). In terms of resolution and indexicality, the data that Facebook collects aims to be as detailed as possible, making each user as uniquely identifiable as possible for direct target marketing. Finally, Facebook ensures that its data are relational and flexible to be able to offer marketers and data brokers the ability to connect users and to change how data are collected. It is the characteristics of big data and the context within which they are created which makes informed consent difficult, especially when considering their real-time nature, their velocity, and their volume.

In their complaint to the Office of the Privacy Commissioner of Canada (OPC) in 2009, the CIPPIC noted this lack of fully informed consent for social media users, alleging that because of the default privacy settings Facebook uses, an opt-out rather than an opt-in system of consent, means that users are rarely aware of changes in how their data might be used (CIPPIC, 2009, p. 18). The OPC found that on the default privacy settings, Facebook was doing a reasonable job of maintaining default settings that made sense, however, Facebook could benefit from making the initial consent process clearer

to users so that they are aware that they can change their privacy settings should they wish to do so (CIPPIC Complaint, 2009, p. 25). As we shall see in more detail in the fourth chapter, consent and big data is not clear cut.

2.3 Defining "Platforms"

Facebook and other social media giants have consistently presented themselves to regulators as "platforms", but these are rarely defined, which is unfortunate since regulators regulate based on how the companies and their technologies are defined. For example, a broadcasting company and a telecommunication company are each regulated differently, while social media companies represent themselves in ways to advocate for the forms of regulation (or lack thereof) that best suit their interests. As Tarleton Gillespie (2018) eloquently puts it, "*platform* is a slippery term, in part because its meaning has changed over time, in part because it equates things that nevertheless differ in important and sometimes striking ways, and in part because it gets deployed strategically, by both stakeholders and critics" (p. 18).

There are several definitions of a 'platform', some are rooted in platform studies, which is part of digital media studies, which examine the hardware and software configurations of computational systems. For example, Ian Bogost and Nick Montfort (2009) define platforms, from a platform studies point of view as "a computing system of any sort upon which further computing development can be done" (2009, p. 2).

In *The Politics of Platforms*, Tarleton Gillespie (2010) identifies four broad definitions of a platform. Like Bogost and Montfort, the first broad definition is a computationally oriented, whereby a platform is "an infrastructure that supports the design and use of particular applications, be they hardware, operating systems, gaming

devices, mobile devices or digital disc formats" (Gillespie, 2010, p. 349). The second category is also the oldest definition of a platform, states that it is an architectural structure, such as a physically raised surface upon which people can stand. The third category is figurative, with "the material 'platform' for physical industry becomes a metaphysical one for opportunity, action and insight" (Gillespie, 2010, p. 350). Gillespie's last definition stems from politics[28], a politic platform, which is a collection of promises, beliefs, and issues that a politician or a political party is for or against. A platform can therefore also be cast as a neutral stage from which to broadcast ideas. In adopting this latter definition, a platform becomes represented as a discursive space that is somewhere, open and accessible to all who desire to use it (Gillespie, 2010, p. 351).

Facebook infers that it is analogous to a neutral political platform, especially when speaking to regulators and users. By doing so Facebook suggests that they are beyond reproach, and should not be regulated according to the norms of behavioural regulation, nor content regulation, simply because they are solely a platform for others to share their own content. This definition suggests they are neutral and therefore Facebook should be absolved of the responsibility for whatever people (users) do on its platform.

Facebook does, however, influence user content on its platform, as is part of its business model which is the generation and use of personal data and social media data that users post. Even if Facebook were truly and completely neutral regarding the content on its site, it nonetheless is always using the data of its users, making it more than a simple platform upon which speech happens, and instead it is a place of exchange of

[28] In this instance, political does not refer to the actual political leanings of social media platforms, but rather to the notion of political neutrality.

services for goods, the goods being user data which Facebook can reuse and resell. The distinction between how Facebook deals with content on its site and the ways in which it mobilizes the personal and user data it gains from user interaction with its site is key to understanding how to accurately define what a platform is. In *Custodians of the Internet*, Gillespie defines platforms as online sites and services that,

a) host, organize and circulate users' shared content or social interactions for them;
b) do not produce or commission (the bulk of) that content;
c) are built on an infrastructure, beneath that circulate information, for processing data for customer service, advertising, and profit (Gillespie, 2018, p. 18).

By this definition, Facebook stages content that is a computational foundation that third parties can build on. Facebook's platforms for third-party applications such as *Workplace*, for example do just that, as,

> Workplace is a platform built on the same infrastructure as Facebook Platform and Messenger Platform. This means that developers can use familiar technology like Graph API and Webhooks to build powerful integrations between Workplace and other enterprise tools (Facebook, 2020).

This includes "Third Party Apps that allow Independent Software Vendors (ISVs) to integrate their Software as a Service (SaaS) and Platform as a Service (PaaS) products with Workplace. Once reviewed and approved by the Workplace team, these apps can then be installed by any Workplace customer to deliver valuable automation" (Facebook, 2020).

The systematic and as comprehensive as possible collection of personal data is simultaneously 'baked into' its infrastructure and business model – as it is in Facebook's best interest to actively encourage third parties to use its platform, and by extension its access to personal and user data, to develop applications. As seen, Facebook is hardly a

neutral platform: it is designed, owned, and structured in very specific ways to maximize the collection, retention and use of personal and public user data that its massive audience of users provide. Moreover, it is hardly neutral with respect to the structuring of the content on its platform. It actively curates and moderates user generated content while tweaking all sorts of things to tailor people's experience of Facebook. As Gillespie explains:

> the moment that social media platforms introduced profiles, the moment they added comment threads, the moment they added ways to tag or sort of search or categorize what users posted, the moment they indicated what was trending or popular or featured – the moment they did anything other than list users' contributions in reverse chronological order – they moved from delivering the content for the person posting it to constituting it for the person accessing it (Gillespie, 2018, p. 42).

And therefore, social media platforms like Facebook are not neutral in the way that ISPs might be. Whereas ISPs are *required* to be impartial in terms of the services which are accessed, Facebook is better seen as actively curating and editing its service and, therefore, functions in a manner more like a broadcaster or publisher. Indeed, some suggest there is merit in defining social media platforms as broadcasters to make them responsible for the content they make available and circulate, much like the way broadcasters are (Napoli, 2019; McKelvey, 2018). It is ill-advised to characterize social media platforms in this way as they constitute a new hybrid form of media company and are, by design, heterogeneous in terms of functions, design, business models and activities. Social media can be understood, then, as something that is "distinctly neither a conduit nor content, not only network or only media" (Gillespie, 2018, p. 41). Instead, they are something in between. As such, social media need to be regulated according to their unique characteristics, rather than trying to force-fit them into one pre-existing category or another.

Philip Napoli (2019) has examined how social media platforms have actively avoided being considered as media companies. According to Napoli, social media platform companies most often want to be thought of as technology companies, as first and foremost, they point to the fact that social media platforms are not content creators. Since they are only providing access to content created by others, so the argument goes, they cannot be considered as media companies in the way that broadcasters or publishers are. Napoli challenges this argument by pointing out that "both cable television and satellite industries were built entirely on the foundation of serving exclusively (at least initially) as distributors of media content" (Napoli, 2019, p. 9) but are currently thought of as media companies. The comparison to television is two-fold, first, the distribution of content has historically been thought of as falling under the realm of media companies, and even though a company may begin strictly as a distributor of media, they will often vertically integrate to become more involved with the content curation or creation. Given that Facebook is a highly curated application whose algorithms control what media each user sees, going far beyond the simple delivery of content, and the fact that Facebook is increasingly looking into ways to integrate its own content creation processes[29], the argument that Facebook is solely a technology company is difficult to uphold.

Napoli's second argument is that social media companies claim that their staff consists strictly of technology experts, engineers, and computer scientists not media and entertainment industry creative personnel and editors. To this, Napoli counters that almost all the current media companies and sectors, such as radio, were new technologies

[29]*Facebook exploring creation of its own original video content* by Darrell Etherington from Techcrunch https://techcrunch.com/2016/12/14/facebook-exploring-creation-of-its-own-original-video-content/

at some point, which meant that the staff at these companies were initially also predominantly technically leaning in their skill sets (Napoli, 2019, p. 10).

Social media companies also make another argument that is closely related to the second and has to do with the claim that they do not employ human editorial staff to approve or disapprove of the content that is posted to their platforms. The stated lack of human intervention - although as Gillespie (2018) demonstrates, there is in fact a lot of human intervention that happens in the process of content moderation on social media sites - is meant to indicate that the algorithms that perform the sorting and prioritization of content are neutral and lacking in editorial oversight in ways that other media companies are not. Napoli responds by explaining that "simply because the mechanisms for exercising editorial discretion – for gatekeeping – have changed does not mean that the fundamental institutional identity of the gatekeepers should be recast" Napoli, 2019, p. 12). Indeed, the process of algorithmic choice is always based upon human choices that go into creating and training the algorithms, meaning that algorithms are by no means any more neutral than humans are.

Napoli also girds his arguments for why social media platforms are media companies by pointing to their advertising revenue and the centrality of consumer data to their core business models. In other words, social media companies are competing with traditional media companies for the core of the media business: advertising revenue. He explains that "being in the business of providing content to advertisers while selling those audiences to advertisers is a defining characteristic of the media sector" (Napoli, 2019, p. 14). Therefore, Napoli argues that when thinking about the regulation of social media

companies, it is important to simultaneously take a technology-centric and a media-centric view, rather than simply one or the other.

For the purposes of this thesis, I define social media platforms in a similar way to how Gillespie and Napoli define them – as hybrid companies wherein "users entrust to them their interpersonal "tele" communication, but those contributions then serve as the raw material for the platforms to produce an emotionally engaging flow, more like a "broadcast"' (Gillespie, 2018, p. 41). The term platform here will lend itself to describing the technical nature of social media, while also indicating that platforms act as moderators and curators of content, and by extension, speech. This also more resembles their business model, which is the collection, aggregation, and use of personal data. In many ways I will be defining social media platforms as a combination of ISPs and broadcasters – considering them to exist within a space that bridges the previously much clearer divide between these two service sectors[30]. In this case here, it becomes unhelpful to argue whether social media should be regulated as a technology company or as media company, as the fundamental existence of social media platforms break conventions and need to be addressed within their own unique set of circumstances and operational realities that require a regulatory framework that takes both technology and media into account. When it comes to data protection and privacy issues on social media platforms, trying to classify social media as either an ISP or a broadcaster does nothing to help in

[30] Although in Canada, these two different sectors (Broadcasting and Telecommunications) are often owned by the same companies, making the distinction between services more complicated as companies are increasingly vertically integrating between content and service provision. As Winseck explains "vertical integration is where communications companies own media content companies. Current levels of vertical integration are exceptionally high in Canada by both historical standards and international standards. Indeed, the scale of vertical integration doubled between 2008 and 2013 and by 2018, four vertically integrated communications conglomerates in Canada had come to account for 56.5% of the $86.2 billion network media economy: Bell, Rogers, Shaw (Corus) and Quebecor (Winseck, 2019, p.ii).

the application of the three main modes of regulation to social media and instead serves to obscure the complex and differing ways that platforms operate.

2.4 From Content Regulation to Content Moderation? What to do about "Lawful but Awful" content

Content focused regulation is constructed around and constrained by the principles of freedom of expression in Canada (Charter of Rights and Freedoms, 1). While content regulation is the focus of broadcasting style regulation, it does not play a large role with respect to either telecommunications or publishing. Content regulation has been the focus for discussions about how to regulate Facebook in many quarters, with many people examining how hateful and harmful content on social media platforms are a destructive force in a peaceful and democratic society (Mueller, 2015; Keller, 2018; Vaidyanathan, 2018).

In many ways, content regulation has probably dominated the narrative around social media regulation more than it ought to, sidelining structural and behavioural approaches in favour of a moral 'panic-esque' discussion of what is acceptable speech versus unacceptable speech when it comes to platforms. This focus tends to go far beyond what is lawful and permitted speech to lay great emphasis of what might be lawful but *harmful* speech that should be monitored and, in some cases, removed by social media platforms. It is a question of how social media platforms should perform content moderation, something that they already do to try and maintain a certain level of user friendliness and make their platforms a place where most users feel comfortable. However, for the most part, this is self-regulation by the companies themselves rather than content regulation by the Canadian government. It is also a question of whether content moderation should go beyond taking down just harmful content, in lieu of how

Facebook currently takes down innocuous pictures of breastfeeding mothers under the claim of inappropriate nudity – a topic of debate which has been ongoing for many years (Gillespie, 2018, pp. 145-169).

Gillespie has examined how social media platforms moderate, curate, and in some limited instances, generate content on their platforms. As discussed earlier, Gillespie points out that while there is a common myth that platforms are neutral, simply providing a space where content can be posted and circulated without any oversight, the truth is that platforms have always moderated user activity in one way or another (2018, p. 5). Most, if not all, social media platforms have terms of service, which users must agree to if they wish to use a social media platform, as well as community guidelines, both of which detail the rules that the platform has for its users to abide by (Gillespie, 2018, p. 46). The wording of these documents varies, but their main purpose is to provide platforms' policy teams with the justification for removing certain content. Furthermore, these documents are meant to ensure that the platform remains welcoming to its users by encouraging users to act in certain ways on the platform, since it is in the platform's best interest to moderate extreme content that could chase users away. Because platforms do not have the capability to monitor what content is posted by users to their sites, in part because of the sheer amount of content uploaded every minute of every day, in the way publishers ensure that they have had a say in what goes out to the public,[31] they must instead rely on other methods to ensure that the content being posted on their systems follow their

[31] It should be noted that social media companies could, if they so desired, implement a system like publishing, wherein they reviewed and approved content before publishing it to their platforms. However, this would change the entire structure of how content exists on social media platforms and would not necessarily be a change for the better. If social media were commissioned and or paid for, that would imply that the companies own the content as a publisher.

community guidelines. These methods include self-reporting by members of the platform's community (community flagging), who flag content that violates the platform's community guidelines, such as terrorist rhetoric, by employing artificial intelligence to identify offending content, and with human editors hired specifically to review content posted to platforms, often after being flagged as not aligned with the company's terms of service or community guidelines by community flaggers or AI systems (Gillespie, 2018).

A core reason for social media platforms to monitor and moderate their content is because of copyright laws. Unlike speech, copyright legislation offers a clear legal mechanism to ban specific types of content with a mechanism requiring platforms to remove copyrighted content brought to their attention. Disney, for example makes frequent requests to have their copyrighted content removed from social media platforms, and it leverages copyright laws very effectively to ensure that users do not post or use their copyrighted content without a licence to do so.[32] Yet, social media companies are not as susceptible to copyright laws as other media, such as broadcasting. Section 230 of the Communications Decency Act (CDA) does two things for social media. First, it allows them a safe harbour from being liable for the copyrighted content that appears on their platforms. Yes, they are required by copyright law to respond to copyright takedown requests, but they are protected from taking legal responsibility for the copyrighted

---

[32] Some examples of Disney leveraging copyright can be found in the following articles: *Disney vs. The Public Domain: How Mickey Mouse Continues to Protect His Copyright*, at https://lucentem.com/2018/12/05/disney-vs-the-public-domain-how-mickey-mouse-continues-to-protect-his-copyright/, *Disney and Lucasfilm suing local business for copyright infringement* at https://insidethemagic.net/2019/12/disney-lucasfilm-suing-local-business-ba1/, and *Irony Alert: Disney (Yes, DISNEY!) Whines About 'Overzealous Copyright Holders'*, at https://www.techdirt.com/articles/20180815/01040040434/irony-alert-disney-yes-disney-whines-about-overzealous-copyright-holders.shtml

content and are absolved from the responsibility of proactively moderating content on their platforms. However, if a social media platform does content moderation, then, under Section 230, the CDA and copyright law can hold them legally accountable for the content that appears on their platform. It is this aspect of social media content regulation that is most often considered a problem, because it encourages social media companies not to moderate content on their platforms in any official capacity. Calls for the modernization of Section 230 ask to mandate social media platforms regulate specific types of content or risk losing their immunity from liability of they do not. Similarly, in Canada, there is a call is for new laws that mandate Facebook and other social media companies to moderate certain types of content that Canadians deem unlawful or harmful.

Questions arise in this context as to what is permitted speech and what is not? In Canada, there is protections against hate speech (Criminal Code of Canada, Section 316, 351), which could be used to form the basis of content regulation for social media, just as it does for broadcasting and publishing sectors. Even so, this approach would be limited in scope, because as Daphne Keller (2019) indicated, "the first cost of strict platform removal obligations is to internet users' free expression rights" (p. 2). While Keller writes about the US, where free speech is a contentious subject, this mode of content focused regulation calls for government to mandate the monitoring of speech and is therefore something that is recognized as being potentially dangerous and problematic in most democratic societies, including Canada. In addition to this limit of speech by the governments through regulation, Keller notes that even the threat of content liability has the possibility of pushing social media platforms into over-removing content in the hopes

that they do not get caught with illegal content on their sites.[33] Keller discusses the tension between platforms enjoying a certain immunity against illegal content, and therefore being accused of not removing enough content, and the fact that many platforms already moderate their content and will take many, if not all removal requests at face value, even if they end up removing speech that is Constitutionally protected (Keller, 2018).

Keller also identifies the tensions between different countries and their varied approaches to regulating social media platforms. Joel Reidenberg (2005) also does so, he specifically refers to jurisdiction, what the global nature of social media platforms means for national borders, and what the technological methods to address these challenges might be. Reidenberg identifies how some internet proponents have "long sought to divorce the applicability of sovereign laws from their online activities" (Reidenberg, 2005, p. 1952). While these proponents have become less vocal over time, the general approach that social media platforms take to their online undertakings furthers this notion of separating what happens on the internet from the rules of physical locations. Although rather hypocritically, social media still invoke the rules of physical locations when it suits their purposes, as we will see during the ETHI Committee hearings when the CEO of Facebook Canada, Kevin Chan, claimed that Canadian user data hosted in the US should be subject to US privacy laws, not to Canadian ones. There have been other cases where

---

[33] This is the main issue within the breastfeeding community, where Facebook routinely removes breastfeeding pictures due to them being flagged as nudity, (*https://www.wired.com/2012/02/facebooks-continued-removal-of-breastfeeding-pictures/. https://www.washingtonpost.com/news/the-intersect/wp/2015/02/26/facebook-is-embroiled-in-yet-another-breastfeeding-photo-controversy/. https://www.dailymail.co.uk/femail/article-4650418/Facebook-user-ordered-remove-photo-breastfeeding-mum.html).*

content on social media platforms appear in one country while being hosted in another country, creating a situation where, as Keller has noted before, the social media platform abides by the rules of the more permissive country — often the US — where the content is being hosted rather than where the content is accessed.

To combat the potential for government censorship or for platforms to over-censor themselves because of regulatory fears, Annemarie Bridy (2018), as well as Citron and Witters (2017), propose that section 230 be modified – rather than struck down all together – and that the Good Samaritan provision of the Communications Decency Act (CDA) could help fight hate speech and misinformation on social media platforms without creating a situation of over-censorship (Bridy, 2018, pp. 23-24, Citron and Witters, 2017, pp. 12-16). The concept of the Good Samaritan is once again based on the regulatory situation in the US, as the CDA does not apply directly in Canada. However, something like it could be used as a method to ensure that content focused regulation does not infringe on the freedom of expression of people in Canada if it were adapted to the Canadian context. The Good Samaritan clause is one that is "intended to protect and promote good faith content moderation at the Internet's edge" (Birdy, 2018, p. 198). This approach would explicitly relieve "service providers of any obligation to adopt content moderation policies that are coextensive with the protective reach of the First Amendment" (Birdy, 2018, p. 209), while also allowing them to moderate content in good faith for the benefit of all users on a particular platform. Strengthening the Good Samaritan provision along the requirements of good faith moderation could go a long

way to normalizing the moderation of harmful content[34] without forcing social media to be held fully responsible for the content, which might push them towards restricting access and infringing on free speech and freedom of expression alike in their attempt not to be held liable.

A Good Samaritan type of provision for content available to Canadian audiences could potentially take the form of legislation that aligned as much as possible with a US Good Samaritan interpretation of section 230, with some added protections to account for the more restrictive speech laws that come with freedom of expression in Canada. While it falls outside the scope of this thesis, considering how content creation is done and how user interaction with content affects the habits of data practices on social media platforms could help to better inform a holistic approach to privacy and data protection regulation for social media platforms.

2.5 Regulatory Considerations: Ways to Address the Current Concerns Around the Cambridge Analytica Scandal

There are many aspects of regulation to be taken into consideration when contemplating how Canada ought to be regulating social media. This includes understanding the unique historical situation of Canadian regulation, as well as because most social media platforms are not based in Canada, which makes Canada much more reliant on US regulation for the social media sector than it is for the other media sectors which are based within Canadian jurisdiction. Building on this unique aspect of Canadian regulation, is the identified need to align Canadian privacy policy and regulation with the

[34] In a more structured and formalized way than is already carried out by the platforms of their own volition as explained by Gillespie (2018).

EU GDPR, a more global approach to Canadian legislation and to harmonize privacy policy across the world, which is better attuned to the global nature of social media. The ability to work across jurisdictions with other regulating bodies can ensure that social media companies are regulated across the board, rather than allowing them to self-regulate within certain contexts. Moreover, social media regulation cannot happen in isolated legislative spheres, and while it may be tempting to focus on one mode of media regulation over another, all three modes will need to be considered and implemented in tandem to better account for the nebulous and layered aspects of social media platforms and their business practices. This includes the content focused mode of regulation, and although it is not the focus of this thesis, it remains important to recognize that all three modes have their merit and their applications in privacy and data protection. Finally, it is important to acknowledge that social media platforms do not exist inside of a vacuum when it comes to the ecosystem of privacy and data protection. While the focus here is on social media platforms, Canadian regulation does need to consider that there are many actors within the data market – such as data brokerage companies – and all proposed regulation should be made applicable not only to social media companies, but to these other actors as well. This will be revisited in chapter four.

Chapter 3: Called it: The CIPPIC Complaint Ahead of Its Time

3.1 The 2009 CIPPIC Complaint with the OPC

In 2008, long before the Cambridge Analytica data breach scandal broke in 2018, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) filed a complaint with the Office of the Privacy Commissioner (OPC) under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). CIPPIC's complaint raised prescient concerns about how third-party applications access Facebook's platform, and consequently to its users' personal and public facing data. Indeed, the issues it raised were strikingly like those at the heart of the unsanctioned use of Facebook/Cambridge Analytica data breach in 2018. Ahead of its time, the complaint was filed in May of 2008 and resulted in an investigation by the OPC for which both Facebook and CIPPIC presented. The OPC's response to CIPPIC's complaint with Facebook was overseen by

Elizabeth Denham, who was the Assistant Privacy Commissioner at the OPC between 2007 and 2010 and the Information and Privacy Commissioner for British Columbia between 2010 and 2016. She is now the UK Office of the Information Commissioner, where she has led investigation of the Facebook/Cambridge Analytica case.

The OPC's investigation in 2008 and their subsequent report in 2009 raised several key issues including 24 allegations about 11 distinct subject areas. The first concern revolved around the collection of the date of birth information of Facebook users, which the CIPPIC alleged should not be a precondition to register for the Facebook service (OPC, 2009, p. 10). Secondly, the CIPPIC alleged that the default privacy settings that Facebook had preselected, allowed for the capture of too much personal information and was an opt-out system, rather than an opt-in system, meaning that consent to the collection of the data was not an informed form type of consent as it could be (OPC, 2009, p. 10). Building on the inappropriate collection of personal data and default privacy settings, the CIPPIC stated that Facebook was not adequately informing users about the ways in which it was using their data for advertisement purposes (OPC, 2009, p. 28). Similarly, the CIPPIC alleged that when Facebook was using personal data for new purposes not initially stated upon the user signing up for the account, Facebook was not adequately informing users of how their data would be used in new ways and with other organizations (OPC, 2009, p. 55). The same claim was made about the collection of personal data from sources outside of Facebook, where, once again, Facebook failed to properly inform users of what personal information would be collected about them from outside sources (OPC, 2009, p. 57). As well, the CIPPIC argued that Facebook was not obtaining consent from non-users for the data that users were uploading, such as pictures

wherein the non-users could be tagged with their names (OPC, 2009, p. 70). Furthermore, Facebook did not explain how it monitored its site for anomalous activity in its privacy policy, therefore monitoring was not something that users were able to consent to (OPC, 2009, p. 84).

A similar consent related matter, but slightly more complicated, when it came to third-party applications, the CIPPIC alleged that Facebook's operations clashed with its obligations under PIPEDA in several other ways. For instance, the CIPPIC argued that Facebook did not adequately inform its users about how third-party applications were using user data and that it was allowing third-party applications access to user data that went beyond reasonable use. It also argued that Facebook was not allowing users to easily opt out of third-party applications that accessed their personal data, in addition because they were not adequately safeguarding user data from third-party applications by not assuming responsibility for the data that third-party applications were taking and by not having any sort of oversight over third-party applications (OPC, 2009, p. 37).

The next set of concerns were related to how users could deactivate or delete their accounts. According to the CIPPIC, while Facebook allowed people to deactivate their accounts, it did not allow them to delete their accounts. Therefore, people could not fully remove their data, which is something that Canadians have the right to do (OPC, 2009, p. 58). It also included accounts of deceased users being kept active without Facebook having obtained meaningful consent from the users before doing so (OPC, 2009, p. 65). The CIPPIC also alleged that Facebook did not have proper safeguards when it came to users logging in through devices that were not their own. As a result, the cookies used by Facebook Mobile meant that if a user did not explicitly log off, let us say on a friend's

phone, their account remained available on their friend's device, even if that user subsequently changed their password (OPC, 2009, p. 78).

Finally, the CIPPIC alleged that Facebook was falsely representing itself as solely a social networking site when in fact it was engaged in other activities that were not clearly explained. The most notable activity in this regard was, of course, Facebook's advertising practices which involved the production and support of content that was not user generated and that third-party applications were central to how the whole platform operated, all of which went beyond the role of simply hosting user content. Furthermore, the CIPPIC argued that Facebook was misrepresenting users' level of control over their personal information. All these considerations, according to the CIPPIC, put Facebook in contravention of PIPEDA (OPC, 2009, p. 88).

The investigation concluded that some of the complaints raised by the CIPPIC were without merit. This was the case, for example, with: new uses of personal information, the collection of personal information from sources other than Facebook, and deception and misrepresentation (OPC, 2009). Other allegations made by the CIPPIC, however, were deemed to be well-founded. As a result, the OPC recommended that Facebook address the issues of concern. This resulted in Facebook changing some of its practices, not just in Canada but worldwide. This was the case, for example, with respect to the collection of date of birth information, default privacy settings, advertising, and how the company monitors its service for anomalous activities. As a result, "Facebook agreed to describe advertising more clearly and to configure its systems to allow users to more easily find information about advertising" (OPC, 2009, p. 94).

At the same time, there were core issues that Facebook refused to address, for example, account deactivation and deletion, the accounts of deceased users, and the personal information of non-users. Perhaps most importantly here, Facebook also intransigently refused to follow the OPC's recommendation for the stricter control of third-party application access to and use of the service — the very issue that would come back to haunt it — and the rest of us— a decade later in the context of the Facebook/Cambridge Analytica data breach (OPC, 2009, pp. 37-54). In each of these cases, the OPC made recommendations to Facebook that would have aided it to resolve issues and made it in line with PIPEDA. For example, when dealing with accounts for deceased users, the OPC recommended that Facebook simply include information about the practice of using the personal information of deceased users for memorial purposes. However, Facebook chose not to implement this recommendation, as it did not consider such additions to the privacy policy as necessary under law (OPC, 2009). Because the OPC lacked, and still lacks to this day, the proper enforcement powers to impose solutions to the well-founded issues within the complaint, all the OPC could do was try and follow-up with Facebook and attempt to work out solutions with them through negotiation.

The final report from the OPC in response to the complaint, the *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*,[35] is the subject of this chapter. Through an examination of this report, I can delve into the concerns and issues that the complaint addressed, discuss the

[35] Referred to hereafter as the *OPC Report*.

recommendations that the OPC provided to Facebook at the time, and examine which recommendations Facebook chose to accept or dismiss. Specifically, by focusing on the part of the complaint regarding third-party application access to the Facebook's platform reveal key issues that would re-emerge a decade later, which has gained worldwide attention by scholars, policymakers and regulators deeply concerned about the Facebook/Cambridge Analytica affair. One associated with access to the Facebook platform to serve the campaign interests of those driving the Brexit campaign in the UK, the 2016 election of Donald Trump in the US, among other examples in other countries.

This complaint provides clues as to how to regulate Facebook now, as it can be compared to the recommendations by the House of Commons Committee on Access to Information, Privacy and Ethics (ETHI) Committee on the Cambridge Analytica data breach, nearly ten years later (ETHI Committee, 2018). The fact that Elizabeth Denham, then the Assistant Commissioner at the OPC and now the head of the Office of the Information Commissioner in the UK, played a star role in both cases is also of historical significance. This chapter will also examine how the OPC's recommendations – both past and present – fit into the three modes of media regulation, to show how they align with the literature and how the OPC operates in relation to other legislative and governing bodies. A focus on the OPC also reveals its weak powers in terms of data protection and privacy in Canada, most notably their lack of effective enforcement powers.

3.2 CIPPIC and the 2009 Facebook Complaint to the OPC

The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) was founded in 2003 by Michel Geist, professor of law at the University of Ottawa who now holds the Canada Research Chair in Internet and E-commerce Law and

is a member of the Centre for Law, Technology and Society. The CIPPIC is a legal clinic based out of the University of Ottawa that focuses on Canadian policy that relates primarily to information and communication technology and services. As part of its mandate the, "CIPPIC fills voids in policy-making by voicing public interest perspectives to technology policy makers in Parliament, in courts, in regulatory agencies, and in international Internet governance forums" (CIPPIC, n.d.).[36] The CIPPIC has filed many complaints with the OPC and has been involved in many policy, legislative and regulatory processes, including appearing before the Supreme Court of Canada, on matters pertaining to copyright, digital expression, telecommunications policy, data protection, privacy, open information, electronic expression, and consumer protection (CIPPIC, n.d.).[37]

The purpose of the 2009 complaint was to advocate for the more rigorous regulation of Facebook and other internet services in the face of lapses in the protection of personal information by such companies. The multi-faceted nature of the complaint demonstrates how the CIPPIC was thinking through the broader questions of personal access to data, consent, and knowledge for users on Facebook. As the platform grew in popularity, user data were at greater risk of being shared given that Facebook's practices relied on extensive personal data collection, default privacy settings that left most of those data available to anyone else with a Facebook profile and did not (and do not) adequately safeguard personal data from being stolen by third-party applications, hackers and so forth.

---

[36] CIPPIC's mandate can be found at https://cippic.ca/en/about-us.
[37] CIPPIC's involvement with consumer advocacy can be found at https://cippic.ca/en.

3.3 PIPEDA, Privacy, and Consent

CIPPIC filed its complaint with the OPC under PIPEDA. This is Canada's federal privacy and data protection legislation that passed in 2000. It applies broadly to all private-sector companies that collect, store, sell, and use the personal data of people in Canada in any capacity, and requires companies to adhere to a set of guidelines based upon several key principles when interacting in any capacity with personal data. According to the OPC there are 10 fair information principles that "form the ground rules for the collection, use and disclosure of personal information, as well as for providing access to personal information" (OPC, 2021), and these are: 1. accountability, 2. identifying purposes, 3. consent, 4. limiting collection, 5. limiting use, disclosure, and retention, 6. accuracy, 7. safeguards, 8. openness, 9. individual access, and 10. challenging compliance.

It principally covers topics such as what sorts of data can and should be collected about individuals under different circumstances, what commercial purposes they can be used for, and sets out the privacy rights that people can expect with respect to the collection and use of personal data. According to PIPEDA,

> generally speaking, individuals have a right to access the personal information that an organization holds about them. They also have the right to challenge the accuracy and completeness of the information, and have that information amended as appropriate (OPC, 2021).

An important value for PIPEDA is that people have a fundamental human right to privacy and when it comes to collecting data about them, their interactions with service providers should be based on knowledge, consent, and respect for their privacy. However, legislation in Canada does not refer to privacy as a human right, in contrast, for example, to the EU General Data Protection Regulation (GDPR). This has become a

major concern for the ETHI Committee, as will be discussed later in chapter four and in chapter five. To ensure that all Canadians are protected, the principles draw heavily on the central notion of informed consent, wherein individuals have control and autonomy over what their personal data get used for, just as they have power and autonomy over their physical selves. Personal data is seen as just that – a personal and a fundamental part of who we are as people – and therefore data belong primarily to the individual who produces them.

The OPC's mandate is to oversee compliance with both the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal private-sector privacy law (OPC, 2021). At its core, the OPC's mission is to protect and promote the privacy rights of individuals in Canada. As a regulator, the OPC performs different roles, most often working with organizations to ensure that they follow regulations, conduct investigations where necessary, and make recommendations when concerns around personal information are identified.

Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs) (OPC, 2021).

All the principles were addressed in the CIPPIC complaint, however, the following were the most important: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure, and retention, and safeguards. These principles all

relate in some way, shape or form to consent, however, the first four — accountability, identifying purposes, consent, and limiting collection — speak most directly to what is considered meaningful and informed consent under PIPEDA and about how companies ensure they obtain consent from their customers. Accountability is the broadest principle and generally refers to the ways in which a company must set up a privacy management system, designate personnel to ensuring compliance with PIPEDA, and provide information as to how the company protects client privacy and personal data.

In terms of the concept of "identifying purposes", this means that companies must ensure that they are properly informing consumers about what data about them are being collected and explain in detail how these data will be used. Specifically, the company should:

1. Review your personal information holdings to ensure they are all required for a specific purpose.
2. When requesting personal information from a customer, explain these purposes to them, either verbally or in writing. And
3. Ensure that the purposes are limited to what a reasonable person would consider appropriate under the circumstances (OPC, 2021).

In terms of meaningful consent, it means that "people must understand what they are consenting to…. And is only considered valid if it is reasonable to expect that customers will understand the nature, purpose, and consequences of the collection, use or disclosure of their personal information" (OPC, 2021). Meanwhile, limiting collection speaks to the requirement that organizations must only collect and use the data they need to fulfill legitimate and identified purposes, through fair and lawful means.[38]

---

[38] More information on Principle 4 can be found at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_ collection/

As per the principles just discussed, but with a focus on the tangible protection of personal information rather than on how to set up those protections, and explain and obtain meaningful consent, the principle of limiting the use, disclosure, and retention of personal data means that organizations can only use or disclose personal information for the purposes that were identified to the consumer when consent was first obtained. For any additional uses or disclosures, the organization must seek additional consent in a manner that is consistent with the consent they have already obtained.[39] Finally, the principle of safeguards states that all organizations must "protect all personal information (regardless of how it is stored) against loss, theft, or any unauthorized access, disclosure, copying, use or modification" (OPC, 2020). They are meant to do so by implementing well-rounded and properly monitored security measures such as a security policy, user education, and technological protections such as passwords, encryption, firewalls, and security patches.

As a regulatory mechanism, PIPDEA was a good framework for the CIPPIC complaint, especially in relation to its focus on knowledge and consent. Of the CIPPIC allegations that the OPC accepted as having merit, they all shared the common thread that Facebook was not being open enough with its users about what data were being collected, stored, and used and this, in turn, meant that its obligation to obtain meaningful consent was not met. Moreover, when it came to the issue of the re-use of data by third-party applications, PIPEDA was also the right framework under which to raise the concern because the central problem of consent remained.

---

[39] More information on Principle 5 can be found at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/

The OPC also made determinations about sub-principles, most notably principle 4, limiting collection, where "Principles 4.2, 4.2.3, 4.3, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.7, 4.7.1, and 4.7.3 and subsection 5(3)" applied (OPC, 2009, p. 47).

Principles 4.2, 4.2.3, 4.3, and 4.3.2 state that an organization must explicitly identify and set the parameters for which data are being collected before or at the time of collection, and consent must be sought before these data are collected, and that the data seeking organization must, within reason, ensure that they have provided the user with a clear and accurate description of the purpose of data collection, to be able to make consent meaningful (OPC, 2009, pp. 47-48). Principles 4.3.4, 4.3.5, 4.3.6, and subsection 5(3), require organizations to consider how sensitive the data being collected are in the determination of the type of consent to obtain, to ensure that express consent is obtained for higher levels of sensitivity. Also, data collecting organizations must consider what reasonable expectations of privacy are, for example what would Facebook users consider reasonable when data are collected, used, or disclosed about them, for what purposes are they collected, and what is reasonable and suitable in the circumstance of collection (OPC, 2009, pp. 47-48). Finally, principles 4.7, 4.7.1, and 4.7.3 state that a data collecting organization must ensure that all personal data are protected with security safeguards to protect against unauthorized access, disclosure, copying, use, or modification, and security safeguards require include technological measures to protect these data (OPC, 2009, pp. 47-48).

Consent must therefore be obtained for every individual whose data are used before a third-party can access these and Facebook is responsible for ensuring that every user whose information can be accessed is aware of the possibility that a third-party may

access their data and must put in place adequate security to protect that information. Also, the more sensitive the data collected are, the more informed consent matters.

For example, PIPEDA states that data such as medical records or income records are almost always considered to be highly sensitive information, while the names and addresses of subscribers to a mainstream news magazine would not be considered sensitive information "however, the names and addresses of subscribers to some special-interest magazines might be considered sensitive" (PIPEDA, 2000. c.5) under certain circumstances since the context in which data are collected can change the level of sensitivity. Finally, a key aspect of consent and privacy is reasonable use, here companies that use the collected data are meant to use them for purposes that would be reasonably expected in relation to the service they offer. Personal data should not be used or disclosed for purposes unrelated to the primary purpose for which they were collected, unless explicitly agreed to by the user.

Issues with third-party applications using Facebook data are detailed and addressed in Section 4 of the report, which begins by stating that:

> Since May 2007, Facebook has provided third parties with a platform [Facebook Platform] that enables them to create within Facebook applications that users can add to their accounts. These applications, which include such items as games, quizzes, horoscopes, and classified ads, access Facebook's database, but reside on the developers' servers (OPC, 2009, p. 38)

All Facebook users can access and add third-party applications to their profile. These applications are for a wide range of purposes, although many of the most popular ones are small games. Some of the top third-party application games for 2020 include *Candy Crush Saga*, *Farm Heroes Saga*, *Criminal Case*, and *Bejeweled Blitz*.

In its allegations, CIPPIC pointed out that when a user added an application to their profile, they were agreeing to let the application access most or virtually all their personal data, as well as the data of people from their friends list (OPC, 2009, p. 38), even though this could have been limited by unselecting the preselected allowance options when adding an application. Here, users could request that none of their information be accessible to third-party applications by choosing the following option from a preselected list: "Do not share any information about me though the Facebook API" (OPC, 2009, p. 39) but doing so meant that they would not be able to download or use the data seeking application. Because the users of these applications had to allow all access to their data, the full opt-out option was therefore no longer available to those users who had already downloaded these and other related applications. This meant that users were often unaware that this option existed unless they had deleted all the applications they had downloaded and specifically searched for the option to block all applications from accessing their profile.

This means that Facebook platform users are generally unaware of the data they are allowing third-party applications to use, and this is especially the case as default privacy settings are only explained in a section on the privacy settings page of a user's profile. As the report indicated, "the CIPPIC alleged that the language of both the settings page and the overview page were confusing" and it was unclear to users exactly which applications had access to their data (OPC, 2009, p. 39). This raised issues in terms of user consent. It is not enough that a user simply clicks a button to say that they have consented to whatever data collection that the application requires because they may not be adequately informed about how the collection and use of their personal data works. As

seen in the previous section, this is a problem because user consent must be actively informed, meaning that users cannot properly consent to third-party applications accessing their data unless they know exactly what each application has access to, and why the application needs those data to provide the services it provides to users. Thus, when it came to meaningful consent, Facebook was contravened PIPEDA, specifically principles 4.2, 4.2.3, 4.3, and 4.3.2, which stipulate the need for a data collecting organization to obtain meaningful consent for all data collection and use.

Another important issue is that third-party applications not only obtain data from the users who add the application to their Facebook services, but they are also obtaining the information of their Facebook friends. Since Facebook only requires the user who adds the application to consent to the third-party application access to data, the users' Facebook friends have no mechanism to consent to the application accessing their data. Indeed, they do not even click a button to agree to the terms of use of the application, their data are collected simply by being on someone else's friend list. Consequently, people on a friend's list cannot opt to block an application's access to their information in this situation, because even if they personally put their privacy settings to block all applications, these applications may still access their data through their friend's account. This is because the default for third-party applications when accessing friends' data is that the applications have access to all the information that that a normal Facebook user would generally be able to see.[40] Thus, in terms of collecting and using data for

[40] This includes "the preselected general option permits the sharing of a user's name, networks, and list of friends, as well as a further series of optional items. The items preselected are profile picture, basic info, personal info (activities, interests, etc.), current location (city), education history, work history, profile status, Wall, notes, groups the user belongs to, events the user is invited to, photos taken by the user, photos taken of the user, relationship status, and online presence" (OPC Report, 2009, p. 39).

reasonable purposes, Facebook's practice in this instance run afoul of PIPEDA's principles 4.3.4, 4.3.5, 4.3.6, and subsection 5(3), regarding the appropriate uses of personal data, especially what would be considered appropriate use by a reasonable person.

Secondly, these principles require that adequate safeguards be put in place to ensure that data are only used for the purposes to which the user has consented, and that no unauthorized uses, access, or disclosure occurs. These protections must also include technological protection measures, such as passwords and encryption. This is especially relevant regarding social media platforms where privacy and personal data protection mechanisms are predominantly ensured through user privacy settings, meaning that it is up to the company to properly inform their users about what privacy settings exist and how to best employ those settings to meet their desired level of privacy.

In terms of user personal data and privacy safeguards and protections, the CIPPIC complaint included Facebook's Developer Terms of Service which required developers to delete any data they had collected from a user for the purpose of administering an application after 24 hours had passed (OPC, 2009, p. 40). However, the CIPPIC complaint stated that Facebook took no action to protect users' personal data by verifying whether third-party applications were following its Terms of Service. The OPC also discovered that "Facebook has provided no evidence that it systematically screens or audits the activities of application developers" (OPC, 2009, p. 42). Instead, Facebook chose to place that burden on users, thereby relying on users "to identify developers that may be violating the SRR and Platform Guidelines" (OPC, 2009, p. 42). If a user identifies that a third-party application may be in contravention of Facebook's Terms of

Service, Facebook reserves the right to deny that application the use of its platform and can disable any application at any time. However, it is unclear how attentive Facebook had been to user-reported issues regarding third-party applications. In fact, the language in Facebook's Statement of Rights and Responsibilities (SRR) about users states that:

> Facebook requires the Platform Developer to enter into an agreement which, among other things, requires them to respect your privacy settings and strictly limits their collection, use, and storage of your information…… [W]e of course cannot and do not guarantee that all Platform Developers will abide by such agreements (OPC, 2009, pp. 42-43).

Thus, while third-party applications had to agree to Facebook's SRR, Facebook did little to nothing to ensure their compliance. This left third-party applications free to get away with collecting, storing, and using user personal data beyond the specified and limited purposes of the application. Furthermore, if users consent to applications to use their personal data, they do so under the assumption that the applications are following Facebook's SSR, meaning that proper user consent cannot be given to third-party applications when compliance with the SSR is not mandatory and enforced. That, in turn, put Facebook at odds with PIPEDA.

This is how Cambridge Analytica gained access to people's data, data that were later used to sway political sentiment as Cambridge Analytica was a third-party application that took advantage of Facebook's business model and lax oversight of the platform's own SSR and Developer Terms of Service to syphon off data for purposes that went well beyond running the application it had originally launched on the platform. Also, Facebook's lax approach to enforcing its own SSR opened the door for Cambridge Analytica to exploit this weakness.

The OPC 2009 report did state, however, that Facebook added a verification program for third-party applications, whereby for "a fee of $375, Facebook will review an application to ensure that it follows the company's guiding principles" including reviewing how the application treats user data (OPC, 2009, p. 43). These measures were completely voluntary on the part of the third-party application developers (OPC, 2009, p. 39). While it may have been in their best interest for third-party organizations to get this certification and display a certification badge to users, the voluntary nature of this arrangement was far from satisfactory from the perspective of adequately protecting people's personal information, as per PIPEDA's requirements. This is something which would only appeal to a developer whose aim is to follow the guidelines and provide a long-term service to users, rather than to a developer whose main aim is to scrape profiles for information without much concern for the longevity of their application or people's privacy rights.

Since the program is voluntary, it becomes easier to understand how Cambridge Analytica might simply ignore the certification process and hope that users do not report how the application uses data, allowing them to stay in a blind spot in terms of data protection. Regarding security and personal data protection, Facebook's practices contravened the obligations set out in PIPEDA and several of its principles, i.e., 4.7, 4.7.1, and 4.7.3, that required it to have adequate privacy security measures, that they be enforceable and able to demonstrate the ability of protecting the personal data of users, something which Facebook was unable to demonstrate, as seen in their submissions to the OPC.

These three third-party application issues were identified by the OPC and considered to be founded concerns and it ruled that Facebook had not taken the necessary steps during the complaint proceedings to address the issue (OPC, 2009). As the report states:

> Most notably, regarding third-party applications, the Assistant Commissioner determined that Facebook *did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers* (*emphasis added*, OPC, 2009, p. 3).

The OPC also recommended that Facebook implement the following four safeguards and procedures:

1. to limit application developers' access to user information not required to run a specific application;
2. whereby users would in each instance be informed of the specific information that an application requires and for what purpose;
3. whereby users' express consent to the developer's access to the specific information would be sought in each instance; and
4. to prohibit all disclosures of personal information of users who are not themselves adding an application (OPC, 2009, pp. 53-54).

The aim of these recommendations was to reduce the likelihood of applications abusing the system and not complying with Facebook's SSR in terms of personal user data retention, as well as to encourage Facebook to take a more active, responsible, and stricter approach to the oversight of third-party application developers on its platforms. They were also meant to protect the process of user consent and provide users with the ability to actively make choices about sharing their personal data in an informed manner. Recommendation (4) in particular, means that users who did not add applications themselves would be protected from third-party applications accessing their data without their knowledge and consent. In other words, the OPC was saying that third-party

application developers should not be able to use one person's consent to ransack that person's friends list as an additional source of data harvesting.

Despite the OPC's findings and recommendations, Facebook chose to ignore the most important ones related to application developers' ability to use the personal information of users and meaningful consent. Instead, Facebook insisted that it was adequately protecting user data and was not concerned about third-party application access to user data. Specifically, Facebook argued that third-party applications did not have unlimited and unmonitored access to Facebook user data since there were contractual obligations in place through the SRR. In addition, Facebook also made no mention of technological safeguards to ensure that third-party applications did not abuse user personal data (OPC, 2009, p. 50).

It became clear that Facebook could not protect user data, and ten years later, it became clear that the OPC's lack of effective enforcement powers could not prevent the Cambridge Analytica scandal. These same weaknesses persist today and Daniel Therrien and Elizabeth Denham's testimonies, among others, pointed this out at the ETHI Committee as they recommended that the OPC needs more power to enforce PIPEDA to prevent issues such as this from reoccurring.

The recommendations that came out of the 2009 CIPPIC complaint, were more specific than the recommendations made in the final report of the ETHI Committee in 2018, as the ETHI committee stated that Facebook still does not adequately monitor, audit, or hold responsible third-party applications on their platform. Also, the ETHI Committee in 2018, commented on the lack of enforcement power of the OPC and stressed the need for the OPC to be granted greater powers. The findings of the OPC in

2009 and the ETHI committee's 2018 recommendations revealed what politicians and policy makers in Canada have long known about the problems that gave rise to the Facebook/Cambridge Analytical scandal but have done little to rectify those problems and, specifically, to give the OPC the power it needs to hold social media platforms to account. Canada remains behind on what the EU GDPR offers as protections.

In terms of the three modes of communication regulation, the OPC recommendations would be behavioural modes of regulation. In other words, the OPC was not interested in regulating content, or breaking up the company, as Wu might suggest. Instead, the OPC was keen to get Facebook to change its behaviour by making changes in its Developer Terms of Services, its SSR and, by extension, its business model and access the technological capabilities of its computational platform.

These are powerful levers of regulatory influence and control but, in this case they did not work. The lack of OPC power to enforce its recommendations means that even though they have the mandate to administer and enforce PIPEDA, and respond to complaints brought against companies that violate the legislation, they are unfortunately not able to act against these companies beyond providing recommendations. The Government of Canada has been reluctant to grant the OPC with the necessary enforcement powers to ensure compliance with PIPEDA. As we will see further in the next chapter, regulators have increasingly identified that social media platforms do not self-regulate, and that government oversight and auditing may very well be an important part of the solution to many of the issues the Cambridge Analytica scandal brought to light.

Chapter 4: Responding to the Scandal: The ETHI Committee's Inquiry and Recommendations

4.1 The Standing Committee on Access to Information, Privacy and Ethics (ETHI)

When news of the Cambridge Analytica scandal broke in early 2018, the Canadian government instructed *The Standing Committee on Access to Information, Privacy and Ethics* (the ETHI Committee) to examine the origins and nature of the data breach, to identify who was affected, and to produce a report to mitigate future breaches. The ETHI Committee was founded in 2016 to examine and discuss issues related to digital protections, universal access to communications, and personal privacy in Canada. In 2018 the ETHI Committee accepted the motion to examine the Facebook/Cambridge Analytica data breach on March 22nd, 2018, (ETHI, 2018, 3), and on April 17th, of that year, the Committee began its work.

In this chapter I provide a textual analysis of the documents relating to the ETHI Committee's study, entitled *Breach of personal information involving Cambridge Analytica and Facebook*. The study includes witness testimonies, submissions the committee received during their investigation, the transcripts of the meetings, as well as the committee's interim and final reports (See APPENDIX 1). I frame my observations around the three modes of regulation and the literature on media regulation; and relate these to the 2009 CIPPIC complaint especially since the core concerns raised then resurfaced during the Cambridge Analytica scandal. The goal of this analysis is to identify the important themes discussed at the ETHI Committee and assess its final report and recommendations to identify how these might inform a new generation of social media regulation.

4.2 The ETHI Committee Meetings

The ETHI committee spent approximate eight months and held 18 meetings, to study this data breach. The committee produced an interim report titled *Addressing Digital Privacy Vulnerabilities And Potential Threats To Canada's Democratic Electoral Process*,[41] and a final report titled *Democracy Under Threat: Risks And Solutions In The Era Of Disinformation And Data Monopoly*.[42] The Committee's final report detailed 26 recommendations to the Government of Canada, addressing a wide range of privacy issues, with the aim of mitigating the possibility of another Cambridge Analytica data scandal. Another focus for the committee was political parties, their campaigns, and the possibility of democratic interference stemming from opaque data practices. This is

[41] Hereafter in this thesis referred to as the ETHI Interim Report for the sake of simplicity.
[42] Hereafter in this thesis referred to as the ETHI Final Report for the sake of simplicity.

especially important since Canada does not have comprehensive regulation about data use and political parties. Although, extremely important, for the purposes of this thesis, I will only refer to this in the overall analysis of the ETHI Committee's and will discuss it when it pertains to social media regulation in Canada in terms of privacy at the federal level.

During the 18 public meetings, the Committee "heard from 47 witnesses, some of them having testified more than once. It also received two briefs" (ETHI, 2018, 7). These witnesses included academics, regulators, and industry professionals. Of note, there were testimonies from:

- Daniel Therrien, Privacy Commissioner of Canada,
- Damian Collins, a British MP and Chair of the UK House of Commons Digital, Culture, Media and Sport Select Committee;
- Michael McEvoy, Commissioner of the Office of the Information and Privacy Commissioner for British Columbia, and
- Elizabeth Denham, Information Commissioner, UK Information Commissioner's Office.

From Facebook, there were testimonies from:

- Kevin Chan, Global Director and Head of Public Policy, Facebook Canada, and
- Robert Sherman, Deputy Chief Privacy Officer at Facebook.

Although it is also important to observe that neither Facebook's CEO Mark Zuckerberg or COO Sheryl Sandberg appeared at either the Canadian proceeding or its British counterpart, despite being summoned by both committees to appear.

From AggregateIQ, a Canadian-based company affiliated with Cambridge Analytica in unclear ways (ETHI, 2018, 11), there were testimonies from:

- Zackary Massingham, Chief Executive Officer, and
- Jeff Silvester, Chief Operating Officer at AggregateIQ.

Testimony was also obtained from:

- Christopher Wylie, the whistleblower who disclosed the Facebook/Cambridge Analytica breach, and
- Chris Vickery, Director of Cyber Risk Research, at UpGuard, who had found an online depository of information linked to Cambridge Analytica and which Vickery had flagged to the authorities as being a privacy breach issue.

Finally, testimonies from academics included:

- Fenwick McKelvey, Associate Professor, Communication Studies, Concordia University;
- Colin J. Bennett, Professor in the Department of Political Science at the University of Victoria;
- Maurice Stucke, Professor, College of Law, University of Tennessee;
- Taylor Owen, Assistant Professor, Digital Media and Global Affairs, University of British Columbia, and
- Elizabeth Dubois, Assistant Professor, Department of Communication, University of Ottawa.

Two laws were the focus of the ETHI Committee first meeting: The *Elections Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The main thrust of this first meeting was to establish what had happened during the breach, how the various parties were implicated and connected (AggregateIQ, Cambridge Analytica, and the SCL Group), and to explore how regulatory changes might better address the current situation in Canada on data protection and privacy.

4.2.1 Technology Company Testimonies

The first to appear was Chris Vickery, the Director of Cyber Risk Research, at UpGuard, which is a cybersecurity company that helps businesses manage cybersecurity risks. Vickery stated that he first encountered Aggregate IQ's name while looking through *GitHub,* an online code sharing database. The databases owned by Aggregate IQ

only required a user to set up a profile to be able to access its data – which Vickery did only to discover that there were lists of sensitive data easily accessible to anybody with a modicum of effort. He classified this depository of highly personal information as a data breach, since anyone could access the data and used them for any number of purposes. Furthermore, he explained how these data were misappropriated by Cambridge Analytica from Facebook, commenting that "I would classify this as not necessarily a malicious breach, but it was a violation of the expected way in which this data would be handled in that it was gathered under the guise of academic research not to be utilized for commercial or other purposes — and clearly it was" (Vickery, ETHI 99, 2018). While not technically a data breach, it demonstrated how Facebook was irresponsible as it allowed third party applications unmonitored and unrestricted access to its platform.

From a technical standpoint, Vickery explained that SCL Group, Cambridge Analytica, and Aggregate IQ were sharing code and data, with obvious signs of data transfer between these three companies as seen in each of their databases. In his testimony Vickery stated the following:

> So you have SCL and AggregateIQ that supposedly have no relationship but both working with the same code base. Then, further on down in the code base, there is a field that says "client", and written in there is "Cambridge Analytica". Now, I can't see why SCL Group would be saying that Cambridge Analytica is a client of theirs. They basically own Cambridge Analytica. SCL Group is the mother ship on top of that. The only reasonable explanation to me is that AggregateIQ would have been the one putting Cambridge Analytica as the client, then the code being passed to SCL Group, and that just not being changed immediately. There's a little triangle going on there" (Vickery, ETHI 99, 2018).

The links between these three companies suggested that they were all part of the same company.

Daniel Therrien touched upon several key issues in his testimony. First, he stressed that a balance needs to be struck between the need for data in the digital economy and the need for meaningful, informed consent for the collection and use of the personal information the of people of Canada is something enshrined in PIPEDA. Secondly, he expressed the view that artificial intelligence (AI) and big data make obtaining meaningful, informed consent more complicated. According to Therrien, policy makers should examine the definition of consent, and revisit what constitutes normal expectations of consent, rather than defining consent so broadly that it becomes impossible to enforce it in any comprehensive manner. He said that consent under PIPEDA was not defined clearly enough, making the rules around consent murky. Thirdly, he emphasized the need for the OPC to proactively conduct audits on companies instead of audits only being triggered by a complaint. The rational he provided was related to how the OPC had to wait for complaints from an individual or an organization (such as the CIPPIC) to identify potential problems. That, in turn, is a problem "because of the opaqueness of the system, that [complaints] will be rare. That's why I'm saying that part of the solution is also the authority to inspect without grounds, so that we can verify, and order-making and fines would have made a difference" (Therrien, ETHI 101, 2018).

Fourthly, Therrien also wondered whether Facebook had violated privacy laws in Canada along with AggregateIQ. As stated by Vickery, Facebook may have been subject to a breach of the data on their platform through misappropriation, but were they in contravention of PIPEDA by allowing third-party applications to freely access data from its platforms with little oversight or security measures? Therrien, here nods to the 2009 CIPPIC complaint, stating that:

> More specifically, we will be examining whether Facebook's privacy policies actually were too permissive and whether they played a role in the subsequent use of the information by analytics firms to give advice that may or may not have been useful to political parties, among other things. We will also be trying to determine, as I said earlier, whether the recommendations made by the Office before I arrived in 2009 are still applicable in 2018 (Therrien, ETHI 101, 2018).

Because of Facebook's unwillingness to implement the 2009 recommendations made by the OPC, it can be argued that Facebook was also at fault for the Cambridge Analytica scandal; as had it implemented the recommendations, the scandal could have been avoided. Facebook had a responsibility to ensure that the third-parties follow its Terms of Service and Statement of Rights and Responsibilities (SSR) as per PIPEDA. Referring to the 2009 CIPPIC complaint, Therrien reiterated to the Committee that Canada does have a comprehensive set of privacy and personal data protections in place through PIPEDA, but the OPC is hindered by its lack of enforcement power under the legislation. Given this, he argued that a first step towards addressing the concerns raised by the Cambridge Analytica scandal would be to provide the OPC with necessary enforcement powers. Stronger privacy and data protection legislation with the goal of better aligning Canadian privacy law with the EU's General Data Protection Regulation (GDPR) might usefully build on that first step, he suggested.

Finally, Therrien touched on the issue of the dominance of internet companies and their market power and the need for effective regulation to address that market power, especially in terms of data and privacy protection. While he did not comment on what mechanisms were needed to regulate Facebook, he called on the Committee to consider market dominance. He also thought that a different regulatory body might be required to better address issues pertaining to personal data protections and privacy when they intersect across regulatory areas. This, he argued, was because while the OPC is capable

of sharing information with other data protection authorities, both nationally and internationally, it is not well connected to other regulating bodies in Canada such as the Competition Bureau.

Christopher Wylie, the whistleblower who made the Cambridge Analytica scandal public, appeared after Therrien. Wylie worked for the SCL Group, as part of the Cambridge Analytica branch, between 2013 and 2014. In that capacity, he observed how Cambridge Analytica misappropriated data from many different sources to work on targeted advertising campaigns, specifically political campaigns. While he did not personally work on the 2016 Trump campaign, he was very familiar with the *Vote Leave* campaigns in the UK. According to Wylie, both campaigns pulled information and data from a dataset that had originally been compiled by Aleksandr Kogan, collected as part of an academic research project he led at Cambridge University. The data gathered by Kogan was then combined with multiple other sources of similarly misappropriated data.

When asked about the relationships between SCL Group, Cambridge Analytica, and Aggregate IQ, Wylie stated that they were all the same company, with the SCL Group having multiple branches, such as SCL Social, and SCL Elections. To establish themselves in the US, Cambridge Analytica was founded and given access to the intellectual property of SCL Elections. As Wylie explained:

> it acquired not SCL Elections itself, but merely the intellectual property of SCL Elections, so SCL Elections assigned its IP to Cambridge Analytica. Cambridge Analytica, in return, provided a licence to that same intellectual property back to SCL Elections with a second contract that guaranteed that all work from Cambridge Analytica would be performed by SCL Elections (ETHI 109, 2018).

The SCL Group also wished to scale up the size of its operations and to prioritize the development of technology solutions to political campaigns. To help accomplish this, while employed at SCL, Wylie reached out to hire Jeff Silvester and Zack Massingham. While they were interested, they were not enamoured with the prospect of moving to London to join SCL Group. Aggregate IQ, to accommodate them, was established as a technically separate company in Canada. As Wylie explained that the:

> arrangement they had with SCL was that any work that they performed for SCL would then be owned by SCL. The intellectual property that was being developed at the time was then assigned or transferred to SCL. You could think of AggregateIQ as a bit like a franchise (ETHI -109, 2018).

The fact that all three firms were effectively owned by the same company, but registered in different countries under the guise of different regulatory jurisdictions, highlights the need to harmonize regulations across jurisdictions to mitigate these types of data transfers and the circumvention of regulation.

Wylie's revelatory testimony about SCL Group's goals and their work on political campaigns was disturbing considering the targeted marketing they intended to carry out and the behavioural influence they hoped to exert through data-rich psychological profiling. While the influence of psychological profile-driven advertisement remains unclear, and probably not as effective as many in the business of advertisement and marketing, such as Facebook, Google, and even the SCL Group itself claim, their intentions to interfere with democratic processes and spread misinformation were clear.

4.2.2 Facebook Testimonies

The Committee called Kevin Chan, the global director and head of public policy for Facebook Canada, and Robert Sherman, deputy chief privacy officer at Facebook, to give testimony. Their testimony was called to explain what occurred at Facebook, to

examine how Facebook dealt with the breach, including activities to prevent such breaches and misappropriations, and what they had done since to mitigate this from happening since the scandal.

According to Sherman, Facebook investigated the first allegation of Cambridge Analytica's use of their user data, stating that:

> in 2015 we learned from a report in *The Guardian* that a Cambridge University researcher named Aleksandr Kogan had shared data from a quiz app that he operated on the Facebook platform, This Is Your Digital Life, with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Dr. Kogan's app from our platform and demanded that Dr. Kogan and certain other entities he had relationships with, including Cambridge Analytica, delete any information they had received (Sherman, ETHI-101, 2018).

At the time, Facebook was under the impression that the issue had been dealt with although they had no way to verify that Kogan, Cambridge Analytica, and associated entities had deleted these data. Sherman went on to explain that in 2014, Facebook tightened its security vis-a-vis third-party applications by limiting the data that application developers had access to. He also tried to assure the Committee that an application developer today could not access Facebook user data in the way that Dr. Kogan had, thanks to these restrictions. Also, when the 2018 article about the Cambridge Analytica scandal came to light, Sherman explained that Facebook had set limits as to the amount of data that application developers could access. The social media giant had also introduced additional safeguards to ensure that, for example, third-party applications no longer had access to a user data if the user had not used the application in three months. Beyond these data access restrictions, Facebook was also assessing all third-party applications that had access their platform and to user data prior to the restrictions introduced in 2014. The company was also in the process of proposing and implementing

changes to their Data Policy and Terms of Service to provide more information to users about how their data are used and what privacy options they ought to have through their personal privacy controls.

The measures identified by Sherman are important, since many of them align with the recommendations made by the OPC in 2009. But the fact that Facebook resisted implementing these original recommendations then but was implementing them now "on their own", so to speak, suggest a disregard towards the regulatory framework that Canada already had in place under PIPEDA rather than a pro active interest in protecting its users. When asked about what sort of regulatory approaches would be best to help address the issues raised by the Cambridge Analytica scandal, Sherman answered that he thought that the principles-based approach that exists in PIPEDA already provided a strong enough set of privacy protections. In his view, the current regulatory measures and OPC powers were enough, despite it being clear from experience that the OPC's lack of authority to enforce its earlier recommendations had led to this current scandal. In sum, without proper regulation and enforcement powers for Canada's privacy and data protection regulator, the OPC, companies like Facebook will likely only react to problems as they emerge rather than proactively self-policing to prevent problems from occurring in the first place.

The need for stronger regulation, as well as the need to align Canadian privacy policy with the EU GDPR, was reiterated with Kevin Chan's testimony. When he spoke to the question of Facebook's responsibility and accountability towards Canadian users, he noted that Canadian's were served by Facebook Inc., based in California, and that was where Canada must look to for accountability. As Facebook Inc. is not physically located

in Canada, thus the data of Canadian users is hosted beyond its borders, poses challenges for the OPC to exert its authority, as PIPEDA does not have the exterritoriality reach that the EU GDPR does. When questioned about why Facebook implemented EU GDPR and changes to its privacy and personal data protection practices for Canadian as well as for European users, Chan provided no clear answer. Instead, he suggested that Facebook would only implement changes to protect user personal data and privacy if regulation demanded it, and only in the jurisdictions where these regulations were enforced. In other words, this was not so much a jurisdictional problem but one of enforcement, reiterating the problem with the lack of enforcement powers of the OPC and PIPEDA.

The Committee also heard from Aggregate IQ in the testimonies of Zackary Massingham, the company's Chief Executive Officer, and Jeff Silvester, its Chief Operating Officer. They discussed the relationship between Cambridge Analytica and their company, as well as the involvement of both companies in Brexit political campaigns. They denied having any knowledge or involvement in that scandal and were adamant that they had no connections to Cambridge Analytica or the SCL Group. This was despite the information and data of Chris Vickery's discovery that identified the relationship of AggregateIQ as the Canadian branch of the SCL Group on their servers, as well as testimony from Christopher Wylie and as seen in documents that were shown to the Committee. Massingham and Silvester insisted that their work was solely related to targeted advertisement campaigns in the Brexit vote and that they had never worked with Cambridge Analytica or its parent company. When asked about funding from Brexit campaigns related to the Cambridge Analytica scandal, both men assured the Committee that the work they had performed for these campaigns had been above board. However,

they were not able to explain why funding had come to them from two different groups – BeLeave and Vote Leave –coordinating the Brexit vote campaigns under different names but run and funded by the same organizations. Similarly, they were unable to provide substantial information on the type of work they performed for these two groups.

Both the ETHI Committee interim and final reports wrote that the Committee was dissatisfied with Massingham and Silvester testimonies. Both reports also stated that the two did not provide clear information and called into question their intentions. Indeed, as the ETHI Committee's final report states, their testimony "did not concur with the version of the facts presented by the AIQ representatives at that point because their testimony was inconsistent, full of contradictions and contrary to the testimony of several other reliable witnesses" (ETHI, 2018, p. 11). The other witnesses included Christopher Wylie and Chris Vickery, who both identified that Aggregate IQ was a Canadian branch of the SCL Group, which also owned Cambridge Analytica. Elizabeth Denham, Daniel Therrien, and Michael McEvoy also indicated that their respective investigations left them unsatisfied with the Aggregate IQ answers regarding the relationships between Aggregate IQ, Cambridge Analytica, and the SCL Group. Furthermore, the "Committee also observed that AIQ representatives had failed, during a certain period, to cooperate with the investigation of the UK Information Commissioner, Elizabeth Denham" (ETHI, 2018, p.11).

The need for Canadian regulators to audit companies, on short notice and without waiting for a complaint to arise from the public, or a scandal to be widely reported, became clearer after the evasive way Aggregate IQ engaged with the investigation. It became evident that asking a company to cooperate with an investigation was inadequate

to effectively understand the issues and to hold the company accountable for the violations of regulation. Information that a company is willing to share with regulators needs to be verifiable by a third-party to ensure that it is accurate. Regulators also need effective deterrent and enforcement powers.

4.2.3 Testimonies from Regulators

The ETHI Committee also heard from other international and provincial regulators about what they were doing in the face of the Cambridge Analytica scandal, in particular from Elizabeth Denham, Information Commissioner, UK Information Commissioner's Office[43], and Michael McEvoy, Commissioner, Office of the Information and Privacy Commissioner for British Columbia (BC OIPC). Denham started her testimony by outlining what the UK Privacy Commission was doing regarding the Cambridge Analytica scandal. Although at the time, she was not at liberty to discuss the investigation in detail, she could say that it involved "over 30 organizations, including political parties and campaigns, data companies, and social media platforms… Among those organizations is AggregateIQ, which was used by several U.K. campaigns, a company that this committee has already heard from" (ETHI 106, 2018).

The investigation led by the UK ICO, paralleled some of the work done by the ETHI Committee and the OPC. The UK ICO differs from its Canadian counterpart in a very important way, it can levy substantial fines and penalties from companies found to break EU data protection regulations. Denham explained that during the UK

[43] Denham was the Assistant Privacy Commissioner of Canada between 2007- 2010 and presided over the 2009 CIPPIC complaint against Facebook. She has been the UK Information Commissioner at the Information Commissioner's Office since 2016, prior to which she was the Information and Privacy Commissioner for British Columbia.

investigation, while many companies willingly cooperated, there were those that did not and which had, in fact they:

> "attempted to undermine the inquiry by failing to provide comprehensive answers to our questions, refusing to co-operate altogether, or challenging the process… we've been forced to use our statutory powers to make formal demands for information" (Denham, ETHI 106, 2018).

The UK Information Commissioner's Office exerted its powers, and Denham agreed with Therrien that the OPC should be granted far more extensive oversight and enforcement powers than it currently had. As Denham stated:

> the Canadian Privacy Commissioner's powers have fallen behind the rest of the world, so having order-making power, having the ability to levy administrative penalties, civil monetary penalties, and certainly the ability to seize material and to act quickly, I think are really important when we're dealing with global data companies and fast-paced investigations. Even the powers that I have under the current U.K. Data Protection Act were not sufficient in this case. Government has moved really quickly and tabled amendments, which were passed last night, to provide us with even more powers of no notice inspections, streamlined warrants, the ability to make emergency orders, and also criminal sanctions for destruction of records and information (Denham, ETHI 102, 2018).

In the context of global internet companies, Denham argues that it is of utmost importance to have strong regulation across all countries, otherwise these companies can and will move the physical base of their operations and the location of data storage from one country to another to evade regulatory measures where they are strong and take advantage of governments where they are weak. Specifically, when asked about the immateriality of data and if regulators had the necessary capacity to investigate companies, Denham said that even the UK Information Commissioner's Office did not have the authority to effectively regulate these companies. This is due to regulators having to obtain a warrant to search a company, a process that can take up to seven days – too slow when dealing with real-time data. The new EU GDPR has helped streamline

the warrant process to accommodate for quicker turn-around times when dealing with internet companies, and she reiterated the merits of aligning Canadian legislation with the EU GDPR.

In his testimony, Michael McEvoy, Commissioner, Office of the Information and Privacy Commissioner for British Columbia (BC OIPC), explained how the BC provincial privacy legislation – the *Personal Information Protection Act* (PIPA) – contains stronger data protections measures than PIPEDA and, unlike its federal counterpart, requires political parties to report how they use BC user data in their political activities. This provincial legislation supersedes PIPEDA in BC. While the BC OIPC may not have the same enforcement powers as the UK Information Commissioner's Office, McEvoy also indicated that a more robust privacy legislation in BC did not inhibit commercial innovation in the province. McEvoy also highlighted the collaboration between the BC OIPC and the OPC in their investigation into the Cambridge Analytica scandal, but did not discuss details about the ongoing investigation. He did mention, however, that the BC OIPC was providing input to the ETHI Committee based on their dealings with personal data protections and privacy under PIPA.

4.2.4 Academic Testimonies

The Committee also heard testimony from five scholars from four Canadian universities and one in the US.

Professor Colin J. Bennett, Professor in the Department of Political Science at the University of Victoria testimony highlighted how the Cambridge Analytica scandal interconnected several issues, as follows:

> There is the monopoly power of companies like Facebook in the platform economy, the harvesting of data on one's social network through third

> party applications, violations of campaign spending limitations, issues concerning the accountability of targeted political ads, cyber-threats to election integrity, the larger role of big data in our elections, and what I really want to talk about today, which is the role political parties play in data-driven elections and their relationship with our regime of privacy protection (Bennett, ETHI 102, 2018).

Bennett also reiterated the familiar recommendation that PIPEDA ought to be aligned with the EU GDPR at it would not only strengthen the OPC's audit and enforcement powers, but would also strengthen PIPEDA's consent provisions, introduce new provisions for algorithmic transparency, make privacy by default and design a core component of company operations, and categorize data on political opinions as sensitive personal data with stronger protections, amongst other things. While his focus was on political parties, he also discussed issues of structural dominance and like Therrien, did not point to a particular solution to address social media monopolies, but he linked personal data protection and privacy regulation beyond the usual behavioural regulation suggestions.

Taylor Owen, Assistant Professor, Digital Media and Global Affairs at University of British Columbia, delved into issues related to the structural make-up of the digital infrastructure within which social media companies operate, commenting on the nature of the internet and big data, including platform dominance, algorithmic processes, and how data are monetized in social media platform business practices. Specifically, his testimony spoke to how social media are driven by the attention economy, with data being collected and used to gain and retain attention and to drive engagement with online platforms regardless of the ethics behind their collection and use, especially when it comes to the use of data for advertising around politics. For Owen, "democracy requires a grounding of common and generally trustworthy information, and I fear that because of

this structural problem this is slipping away from us" (Owen, ETHI 116, 2018). In essence, Owen is agreeing with others, such as Vaidyanathan, that the private sector, which is based around a profit-driven model rather than a public interest model, is in no position to self-regulate in a way that would promote democracy and there is a strong need for government oversight and regulation (Vaidyanathan, 2018).

Associate Professor, Communication Studies at Concordia University, Fenwick McKelvey's testimony touched on issues of online advertising, international companies, and their practice to offshore data to evade privacy laws, and the data practices of political parties. Specifically, in reference to how international companies deal with data, McKelvey argued that even though these companies might be physically located in a country with more lax privacy laws such as the US, they ought not to operate on that basis in other countries where laws and expectations with respect to privacy are stronger. Yet, without accountability and the enforcement of privacy laws, these companies disregard these regulations. He believes that "these issues can be addressed by adding enforcement powers to the office of the Privacy Commissioner and continuing to support its multi-jurisdictional enforcement" (McKelvey, ETHI 116, 2018). These oversight powers would also be beneficial to concerns related to online advertising and political party use of data as well, as the data collection practices that inform these different activities would also come under the scrutiny of the OPC, making the entire process of data collection and use by all entities in Canada more open and transparent.

In her testimony, Elizabeth Dubois, Associate Professor, Department of Communication at the University of Ottawa, concurred with the other scholars that testified, especially on the point that platform company self-regulation was insufficient.

Dubois also found Facebook's response to the Cambridge Analytica scandal to be lacking as Facebook took no comprehensive proactive measures to ensure that the data accessed by third-party applications would be used in the way in which they were intended; secondly, once Facebook was alerted to the data breach, it did not make this information public, nor did it notify the correct authorities about the breach, and it did not take adequate measures to pursue and shut down the activities conducted by Cambridge Analytica. By choosing to take a reactive approach, and only when the scandal came to light to the public, Facebook demonstrated its inability to self-regulate. Dubois was also highly critical of the opaque approaches to self-regulation, with the public and authorities having no way of knowing what sort of data practices a company were undertaking. Without openness and transparency, companies cannot be held accountable.

Finally, Maurice Stucke, Professor, College of Law, University of Tennessee, described the challenges and risks of data-opolies, a situation wherein a few powerful firms monopolize data flows, enabling them to wield significant power over sizable amounts of personal data. He explained that "in Europe, they're known as GAFA — Google, Apple, Facebook and Amazon. As these firms have grown and power, they have also attracted significant antitrust scrutiny, particularly in Europe" (Stucke, ETHI 119, 2018). In the US, these firms have avoided any sort of substantial focus from regulators. Stucke echoes some key points raised by Wu (2018) and Houser and Voss (2018, 2019), such as the fundamental differences between the European and US approaches to monopolies and anti-trust lie in the ways in which each regulatory system defines threats and potential harm posed by monopolies.

Stucke suggests that once the potential harms of data-opolies are known, the conversation can move towards a consensus of what would be the best policy measures to help mitigate these harms. He listed eight harms resulting from data-opolies that are different from classical monopolies: degraded quality, surveillance, wealth extraction, loss of trust, costs to third parties, diminished innovation, social and moral concerns, and political interference. When it came to classical monopolies, harms were defined more directly in terms of costs to consumers, but here Stucke argues that even though most internet giants provide their services for free, they have much higher potential to cause harm to consumers since the "potential harms from data-opolies can exceed those from monopolies. They can affect not only our wallets. They can affect our privacy, autonomy, democracy and well-being" (Stucke, ETHI 119, 2018). Stucke suggested that antitrust is necessary, but notes that the current global state of anti-trust is not able to adequately address the harms posed by data-opolies, and he calls for there to be greater "coordination with the privacy officials and the consumer protection officials" (Stucke, ETHI 119, 2018).

4.2.5 Lessons Learned by the ETHI Committee

The meetings and testimonies culminated in a final report that provided a detailed overview of the lessons learnt from the Cambridge Analytica scandal. The first was that at the federal level, Canada did not have adequate privacy oversight that applied to political parties and electoral campaigns, creating a blind spot in terms of personal data use in the election process. The second was that there is a lack of general knowledge within the regulatory environment about digital literacy, such as cybersecurity, deep fakes, and misinformation practices, as the technologies that enable these things are

rapidly evolving and changing. Third, social media companies present a regulatory challenge in Canada, even though there is PIPEDA and the BC PIPA, among others, Canadian regulators do not have adequate powers to enforce these regulations.

Based on these set of issues to address, 26 recommendations were identified and made for the Government of Canada to better protect the privacy and personal data of Canadians and to ensure that another Cambridge Analytica scandal is not repeated. The recommendations were organized into four broad categories:

1. privacy legislation and political parties,
2. investment in education on cybersecurity and digital literacy,
3. existing privacy regulation pertaining to social media, and
4. modernizing and strengthening Canadian privacy legislation.

These 26 recommendations are not extensive but do provide a base upon which to build.

4.3 The ETHI Committee Recommendations

The ETHI Committee investigation set out to determine the dangers of personal data use for the purposes of political campaigns, and the first of the four categories covered by its recommendations was privacy legislation and political parties. Recommendations 1, 2, 3, 5, 6, 7, and 26, put forward steps to bring political parties, and any third-party political entities, under existing privacy legislation, such as granting the OPC authority to "conduct proactive audits on political parties and political third-parties regarding their privacy practices" (ETHI, 2018, p. 25) to ensure that the integrity of political undertakings remain intact. There, the OPC would do so under the purview of PIPEDA, as Recommendation 1 calls for PIPEDA to be amended to "subject political parties to it, taking into account their democratic outreach duties" (ETHI, 2018, p. 25). Recommendation 2 similarly calls for the amendment of PIPEDA "in order to subject political third parties to it" (ETHI, 2018, p. 25). As well, some of the recommendations in

this category contained some additional actions to amend other existing legislation, such as the *Elections Act*, to include new measures against the misuse of personal data, including requiring political parties to submit documentation when placing political ads online (ETHI, 2018, p. 39). Recommendation 26, states very clearly that the Government needed to take a holistic approach to ensure that political parties were properly regulated, calling for "measures to ensure that privacy legislation applies to political activities in Canada either by amending existing legislation or by enacting new legislation" (ETHI, 2018, p. 73).

The next broad category under consideration was that of investment in education in areas such as cybersecurity and digital literacy. For instance, recommendations 12, 15, 16, 17, and 18 highlighted the need for a better understanding of the Canadian data economy, online misinformation, and the threats posed to privacy and personal data by cybersecurity – or lack thereof – particularly as it pertained to the Canadian electoral system. These recommendations were straightforward, such as Recommendation 15, which states "That the government of Canada continue studying how cyber threats affect institutions and the electoral system in Canada" (ETHI, 2018, p. 65). When it came to knowledge around online misinformation, the ETHI Committee final report pointed out that across several testimonies, "witnesses were reluctant to make too firm recommendations regarding possible legislative or regulatory measures, noting a lack of information and research on the phenomenon of disinformation and misinformation" (ETHI, 2018, p. 67). To remedy this amongst the public, as well as within governmental institutions, Recommendation 16 states that "the Government of Canada invest in research regarding the impacts of online disinformation and misinformation" (ETHI,

2018, p. 71). Recommendation 17 also states that "the Government of Canada increase its investment in digital literacy initiatives, including for initiatives aimed at informing Canadians of the risks associated with the online prevalence of disinformation and misinformation" (ETHI, 2018, p. 71).

Interestingly, falling under this category, the Committee identified the need to better understand data-opolies and the harms they pose to society. Relying heavily on the testimony of Maurice Stucke, as well as input from Anthony Durocher, the Deputy Commissioner, and the Monopolistic Practices Directorate from the Competition Bureau, Recommendation 12 identifies the need for the Government of Canada to "study the potential economic harms caused by so-called "data-opolies" in Canada and determine if modernization of the *Competition Act* is required" (ETHI, 2018, p. 58). It should be noted that the *Competition Act* relates to anti-trust and in this recommendation, there was some discussion around the issue of monopolies and the need for greater competition regulation to ensure that consumers have choices when it comes to services that collect and use their data. This recommendation touches on the matter of structural regulation rather than behavioural regulation, as it is geared towards changing legislation around ownership rather than the actions that companies take towards their data practices. However, it does not go into detail on the process of modernizing the *Competition Act*, and the issue of structural regulation is unfortunately not covered under any of the other recommendations.

The third category addressed was privacy regulation pertaining to social media. To that end, Recommendations 8, 9, and 10, concern aspects of how Canadian privacy

legislation could be leveraged to provide privacy authorities with the enforcement powers they need to effectively regulate social media.

While many of the recommendations overall pertain to social media, these three recommendations were particularly targeted to deal with some of the key issues identified in the ETHI Committee's examination of the scandal. Recommendation 8, for example, relates to the ways in which social media platform companies should be required to take on certain responsibilities in regard to the content practices on their sites, such as "clearly label content produced automatically or algorithmically; identify and remove the inauthentic and fraudulent accounts that impersonate others for malicious reasons; adhere to a code of practices that would forbid deceptive or unfair practices; and clearly label paid political or other advertising" (ETHI, 2018, p. 41). Likewise, Recommendation 9 calls for greater algorithmic transparency, stating that the Government of Canada should, "enact transparency requirements with respect to algorithms and provide to an existing or a new regulatory body the mandate and the authority to audit algorithms" (ETHI, 2018, p. 41). A central issue with algorithms that was raised over the course of the investigation was that they are too opaque and somewhat inscrutable as a result, and that it is difficult to regulate something that cannot seen or evaluated. By moving towards more algorithmic transparency, the goal is to ensure that any practices that may threaten personal data and privacy ought to be more immediately visible, and therefore more readily be addressable.

Finally, Recommendation 10 addresses the issue of illegal or hateful content on social media platforms, including disinformation and misinformation to attempt to remedy the spread of messages that could jeopardize the integrity of electoral processes.

It calls on the government to enact legislation that would require social media companies to take down such content in a timely fashion, "or risk monetary sanctions commensurate with the dominance and significance of the social platform… allowing for judicial oversight of takedown decisions and a right of appeal" (ETHI, 2018, p. 42). This particular form of regulation is primarily content focused, as it is based on content and not on the action that a company should take, although there are components of behavioural woven in. As was noted in previous chapters, any attempt to regulate speech that is not explicitly criminalized beyond the Canadian Charter of Rights and Freedom protections and remains complicated because of the subjective nature of what constitutes harmful content. Therefore, this recommendation is limited when it comes to what is defined as disinformation and misinformation.

Recommendations 11, 13, 20, 21, 22, 23, 24, and 25 addressed the need for Canada to modernize and strengthen existing privacy legislation either by enacting new legislation or amending those already in place to better address concerns raised by the scandal. Specifically informed by the testimonies of Dunham, Therrien, Stucke, Bennett, and McEvoy, among others, Recommendations 20, 22, and 24 call on the Government of Canada to harmonize Canada's privacy and personal data protection laws with the EU GDPR. Recommendation 20, for example, specifically calls on the government to "immediately begin implementing measures to ensure that data protections similar to the General Data Protection Regulation are put in place for Canadians, including the recommendations contained in the report on Personal Information" (ETHI, 2018, p. 72). Recommendation 22 also calls on the government to ensure that the PIPEDA "be amended to give the Privacy Commissioner enforcement powers, including the power to

make orders and impose fines for non-compliance" (ETHI, 2018, p. 73). This would aid in addressing the ongoing lack of enforcement power of the OPC, as stated in the 2009 CIPPIC complaint and as seen with the Cambridge Analytica scandal. This would provide the OPC with the ability to do more than just make recommendations to organizations that were in contravention of PIPEDA.

To help expedite the OPC's investigations, and based on comments made by Dunham, the Committee recommended that PIPEDA be revised to "includ[e] the power to issue urgent notices to organizations to produce relevant documents within a shortened time, and the power to seize documents during an investigation, without notice" (ETHI, 2018, p. 73). Coupled with Recommendation 23 that calls for the government to grant the OPC "broad audit powers, including the ability to choose which complaints to investigate" (ETHI, 2018, p. 73), this would allow the OPC to conduct investigations in a timely manner that reflects the expedited nature of big data and cloud computing issues such as data breaches more quickly, to ensure that something like the Cambridge Analytica scandal could be mitigated and or resolved more quickly.

Altogether, the ETHI Committee recommendations cover much ground related to the behavioural regulation of social media companies, largely in terms of privacy and data protection and these recommendations address many of the concerns raised by the Cambridge Analytical scandal and could go a long way to ensure it does not reoccur. Although discussed by some during the ETHI Committee investigation, such as Stucke and Durocher, issues of structural dominance were largely missing from the discussion around privacy and data protections that occurred in the wake of the Cambridge Analytica scandal. None of the recommendations put forward in the ETHI Committee

final report meaningfully address substantial structural regulation to mitigate another such scandal. As noted, Recommendation 12 does include a mention of anti-trust, indicating the need to modernize the *Competition Act*, however, no details were provided as to how to go about doing so. This makes some sense since PIPEDA and the *Elections Act* were the focus of the investigation. This oversight means that the recommendations by the ETHI Committee focus on behavioural regulation, a powerful tool against violations of personal data protection and privacy, but this is not enough to address the issues of data collection, storage, and use on social media platforms like Facebook. Despite this gap, the ETHI Committee recommendations provide a solid base to shape and make regulation to avoid future Cambridge Analytica scandals.

Chapter 5: Where Does Canada Go from Here?

5.1 Facebook and Social Media Regulation in Canada

Since the Cambridge Analytica scandal in 2018, Canada has been paying significant attention to questions surrounding privacy and personal data protection on social media platforms and other entities that collect, store, and use Canadian data. The Office of the Privacy Commissioner (OPC), the Office of the Information and Privacy Commissioner for British Columbia (BC OIPC), the Standing Committee on Access to Information, Privacy and Ethics (the ETHI Committee), and the Broadcasting and Telecommunications Legislative Review (BTLR) have concerned themselves with questions about how to better regulate social media platforms so that Canadians have comprehensive personal data protection and privacy laws in place for all their data. Proposals for more robust social media regulation have been put forward by each of these

entities, and if these proposals are implemented, they might aid in ensuring that a scandal such as Cambridge Analytica does not reoccur.

During writing this thesis, The House of Commons tabled Bill C-11 – that proposes to overhaul Canada's privacy laws, and create new legislation to supersede the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The first reading of the bill took place on November 17th, 2020. There are two primary parts to the Bill, the first is to enact the *Consumer Privacy Protection Act*, a bill that promises stronger privacy protections, a more comprehensive definition of consent, and a broader, more internationally minded type of enforcement. The second part of the Bill seeks to ensure that the OPC has more effective enforcement power by enacting the *Personal Information and Data Protection Tribunal Act*. Many aspects of this proposed legislation in part stem from the recommendations made by the ETHI Committee in their final report on the Cambridge Analytica scandal, including proposals to create stronger consent requirements and to give the OPC more enforcement powers.

As such, Bill C-11 will be discussed here in terms of behavioural regulation, as the Bill supports Canadian regulation that focuses on behavioral modes of regulation. This includes requiring organizations to adopt certain protection measures when collecting, storing, and using personal data, and detailing the way organizations are meant to be obtaining consent around their data practices. While by no means a perfect attempt to remedy the concerns raised by the Cambridge Analytica scandal, Bill-C11 does address some. Unfortunately, because the timing of the Bill, I am unable to address these in great depth. The following are however a set of recommendations related to

behavioral and structural regulation derived from the research conducted for this thesis that may strengthen personal data protection and privacy laws in Canada.

5.2 Bill-C11: An Attempt at Privacy Remedies

The new *Consumer Privacy Protection Act* would broadly apply to all organizations that collect, use, or disclose personal information for the purposes of commercial activities, as well as any personal information collected about employees for use in federal work, undertaking, or business, including interprovincial or international collection, use, and disclosure of personal information (Bill-C 11, 2020). Thus, no matter where the information is being kept physically, or no matter where the company is primarily located, the *Act* applies to all personal information that have been collected, used, and disclosed about Canadians during any of their commercial activities allowing for the extraterritoriality of social media to be accounted for under this regulation.

The scope to include all organizations and all types of personal data addresses some but not all concerns raised by the ETHI Committee. For example, focus on commercial activities excludes political parties, considering that electoral campaigns are not defined under the same category as commercial activities. There is no provision in the *Act* that securely brings political parties under the purview of the proposed legislation, meaning that the recommendations made by the ETHI Committee about bringing political parties under privacy legislation have gone unheard. Considering that Recommendations 1, 2, and 3 (ETHI, 2018) clearly called for political parties to fall explicitly under privacy legislation, the crux of the Cambridge Analytica scandal – the concerns over the misuse of personal data in political campaigns – has not been addressed and remains a potential threat to the democratic process.

Under the *Consumer Privacy Protection Act* sections 7 and 8, organizations are accountable for all personal information that is under their control, including any personal information used by service providers on behalf of the organization, and must designate a minimum of one person to be responsible for ensuring that the organization is respecting the *Act*. Under section 9, all organizations must implement a privacy management system that includes the organization's policies, practices and procedures that are in place to meet its obligations under the *Act* (Bill-C 11, 2020). Section 10 specifies that if the OPC requests it, all organizations must provide them with access to all policies, practices, and processes that are included in the privacy management program (Bill-C 11, 2020).

Strengthened enforcement power was identified as a necessary component of privacy regulation during the ETHI Committee proceedings and were featured quite prominently in their recommendations. Dunham, Therrien, and others discussed these issues in their testimonies, and the 2009 CIPPIC complaint with the OPC illustrated how the OPC's lack of enforcement power meant that Canadian privacy regulation was and continues to be ignored by companies. Under PIPEDA, the OPC could only request that companies comply with their investigations, without being able to compel them to disclose the company's data practices. The power to compel disclosure in the new *Act* changes this, making it easier for the OPC to conduct investigations and arguably enabling them to make better, and more informed decisions about when and how a company contravenes the *Act*. Like the ETHI Committee Recommendation 19[44], the new

[44] Which speaks to the need for greater transparency when it comes to organizational data practices, recommending that "that the Government of Canada enact transparency requirements regarding how organizations and political actors, particularly through social media and other online platforms, collect and

powers to compel disclosure would settle some of the concerns around the opacity that most social media companies have operated within regarding their data practices.

Section 12 of the Bill outlines how organizations may only collect, use, or disclose personal information for appropriate purposes. When determining what an appropriate purpose is, organizations must consider the sensitivity of the personal information in question, if the purpose is part of the legitimate business need of the organization or if it goes beyond a need, the effectiveness the personal information will have on meeting a legitimate business need, if there is a less intrusive way to achieve the same purpose, and if the individual's loss of privacy is proportionate to the benefits of the purpose. Appropriate purposes must be determined by the organization before or at the time of the collection of any personal data, meaning that an organization may not collect any personal information at any time without having an explicit reason to do so (Bill-C 11, 2020). If, after collecting certain personal information for one purpose, an organization wishes to use it for a different purpose, they must state the new purpose before proceeding to use or disclose personal information (Bill-C 11, 2020). By requiring organizations to determine appropriate purposes before doing anything with personal data, the *Act* provides mitigation strategies against the misappropriation of data.

The issue with allowing organizations to use personal data for "appropriate purposes" within the context of a "legitimate business need", is that these are terms that lack clear definitions within the proposed legislation, permitting organizations much leeway to define these purposes on their own terms. What an individual might not

---

use data to target political and other advertising based on techniques such as psychographic profiling" (ETHI, 2018, p. 72)

consider a legitimate business need when it comes to their personal data may be seen as legitimate by the organization collecting and using those data. If regulators have no concrete set of guidelines to follow when determining if an organization has been using data for a legitimate need or not, it will be hard for them to determine legitimate and malicious uses of data. This lack of a legitimate business purposes definition also muddies the waters when it comes informed and active consent from individuals, because a company can claim that their data collection practices and use are legitimate, and individuals will have no guidelines to determine the truth of this claim.

Sections 15 to 51 of the Bill are dedicated to defining consent and to detailing exceptions to consent – articulating a much more detailed and comprehensive take on what meaningful consent means and how it is to be obtained in all instances of collecting, using, and distributing personal data. Under sections 15 to 17, all organizations must obtain an individual's valid consent for the collection, use, or disclosure of all the individual's personal information before or at the time of collection of personal information, or at the point that the personal information is going to be used or disclosed for a purpose than was not initially consented to (Bill-C 11, 2020). For consent to be considered valid, all organizations must provide individuals with the following information before or at the time of collection; the purposes for collection, use, or disclosure as determined appropriate purposes, the way that the personal information will be collected, used, or disclosed, any foreseeable consequences relating to the collection, use, or disclosure of the personal information which would be considered within reason to foresee, the specific type of personal information that will be collected, used, or disclosed, and the names of any third-parties that the organization might disclose the

personal information to (Bill-C 11, 2020). Consent is not valid if an organization requires individuals to consent to the collection, use or disclosure of their personal information beyond what is necessary to provide a product or service. Consent is also not valid if it has been obtained under false pretenses, including false or misleading information or practices on behalf of the organization.

In terms of exceptions to consent, sections 18 to 51 provide specific situations that might be exempt from the requirement of valid consent. The following is a list of activities under which organizations are allowed to collect and use personal information without explicit consent:

- an activity that is needed to provide or deliver a product or service which the individual has requested from the organization,
- an activity that is related to due diligence or commercial risk mitigation,
- an activity that is needed for the organization's information, network, or system security,
- an activity that is needed for the safety of a product of service that an organization is responsible for,
- an activity that during which obtaining the individual's consent would be difficult due to the organization not having a direct relationship with that individual, and any other prescribed activity under the Act (Bill-C 11, 2020).

In addition to these activities, the activity must also be within what a reasonable person would expect the personal information to be collected and used for and must ensure that no personal information is being collected or used for any purpose relating to influencing the individual's behaviours or decisions.

This attention to consent and detailed description of the specific instances where there are exceptions to consent will help to strengthen and clarify what counts as privacy and personal information in Canada. As identified during the ETHI Committee investigation by Therrien, the current Privacy Commissioner for Canada, consent needs

to be defined in a meaningful way to provide regulators the opportunity to easily recognize when valid consent has not been obtained so that they can then hold the organizations that are in contravention of the *Act* accountable. Furthermore, by providing ample details on the exceptions to explicit valid consent, companies have better guidelines to aid them in determining what policies and procedures they need to have in place under their privacy management system to properly obtain consent where it is necessary, and where they are free to collect, use, and disclose personal information without explicit consent.

There are, however, limitations to personal consent that rest primarily with an individuals' capacity to provide explicit, and informed consent where nearly all actions that one might take result in some form of data capture. Teresa Scassa (2020), the Canada Research Chair in Information Law and Policy at the University of Ottawa, Faculty of Law, addresses this aspect of Bill-C11, and explains how in most instances, people are more concerned with the service they are trying to access, rather than what data that service is planning to collect from them. She explains that "most people's preoccupation is necessarily with the actual product or service, and not with the many ways in which collected data might be used or shared. They are unlikely to be able to fully grasp how all this might at some future point affect them. Consent is thus largely a fiction" for most (Scassa, 2020 p. 1).

Additionally, Scassa points to the fact that while the language in Bill-C11 promises to make consent a critical focus within privacy regulation, changing the definition of consent for the better, the language around consent in the Bill is not particularly ground-breaking. In fact, in certain instances, Scassa argues that the Bill

makes the situation around consent worse. Specifically, she identifies that a "first problem is that these exceptions are not just to consent, but to *knowledge* and consent. In other words, not only does an organization not need to seek consent for the listed activities, it does not even need to inform the individual about them" (Scassa, 2020 p. 1). By allowing certain circumstances under which an organization does not have to go back to an individual to obtain consent, largely being implemented because of the burden of consent discussed above, the door is open for organizations to define many things as legitimate business needs that do not require direct consent. Considering that the crux of the Cambridge Analytica scandal was that data were initially collected with consent through Facebook, but were thereafter used for different purposes, this aspect of Bill-C11 seems not to have considered the lessons learnt during the ETHI Committee investigation. Namely, that valid consent needs to be ongoing and actively informed because, as Scassa so succinctly puts it, "it is very hard to hold an organization to account for things about which one has no knowledge" (Scassa, 2020 p. 1).

Sections 57 to 61 are concerned with security safeguards for personal information, mandating all organizations to provide physical, organizational, and technological security safeguards to all personal information, making certain that the safeguards are always proportional to the sensitivity of the personal information, and considering the quantity, distribution, format, and method of storage of the information. In the case of a breach of security, organizations must report the details of the breach to the Commissioner, must inform affected individuals in a timely manner, and inform any other organizations that are affected by the breach. Organizations must also keep a record of all breaches and must provide this record to the Commissioner upon request (Bill-C

11, 2020). This requirement of accountability and the need for organizations to maintain a record that is readily accessible to the OPC will help ensure that breaches do not happen, and if they do, any breaches of personal information are dealt with in a timely and transparent fashion and will not drag on as was the case with the Cambridge Analytica scandal.

Finally, to provide the OPC with the necessary enforcement power to ensure that organizations are respecting the stronger privacy principles enshrined in the *Consumer Privacy Protection Act,* and as just described, part 2 of Bill C-11 outlines the Commissioner's powers, duties and functions, and general provisions pertaining to the process of complaints, investigations into complaints, inquiries, and ways to resolve any instances on non-compliance with the *Act*, including penalties that can be imposed on companies who fail to comply with the measures to ensure compliance with the *Act*. Among the OPC's powers is the ability to work with the Competition Commission and the CRTC, as well as with other provincial and international legislative bodies, to compel organizations to participate in audits and inquiries following complaints, and to impose significant fines (Bill-C 11, 2020). These were all important components of regulation identified through the ETHI Committee hearings, and by including these aspects in Bill-C 11, Canadian legislation will be better aligned with the EU GDPR not only in terms of what constitutes valid consent, but also in terms of enforcement.

An aspect of the new enforcement powers that Bill-C11 promises to grant the OPC is the introduction of a Tribunal that is to be created under the new *Personal Information and Data Protection Tribunal Act* that will replace PIPEDA. The Bill states that "the Tribunal has jurisdiction in respect of all appeals that may be made under

section 100 or 101 of the *Consumer Privacy Protection Act* and in respect of the imposition of penalties under section 94 of that Act" (Bill-C11, 2020). The Tribunal is meant to add additional resources to privacy regulators, designating full time members to conduct hearings and proceedings that address raised privacy concerns. It is also meant to create distance between the body bringing complaints against organizations and the body imposing fines. Yet, it is unclear if the introduction of the Tribunal is an improvement to the regulatory situation. Scassa (2021) argues that while the Tribunal could serve some purposes, especially in terms of the separation between complaints and fines, the addition of the Tribunal is more a complication than anything else. Scassa notes that it may not change very much in terms of the general process undertaken by the OPC, especially in cases where no fines need to be imposed. However, she also points to the fact that, "there may also be consequences felt by individuals because of these changes. The Commissioner's findings – not just any orders he might make – are now subject to appeal to the Tribunal" (Scassa, 2021 p. 1). What this may do is undermine the OPC's authority, transferring the final say to determine what constitutes a breach of legislation to the Tribunal, making this aspect of strengthening the OPC's enforcement power rather complicated and precariously uncertain and this may not be an improvement.

Recommendation 1 – Adopt Bill-C 11 as a First Step in the Right Direction

Bill C-11 addresses some of the concerns raised by the Cambridge Analytica scandal and implements several of the recommendations that the ETHI Committee made because of its investigation into the scandal. Should it go through, Bill C-11 would provide Canada with a much more robust behavioural regulatory system and better ensure that social media platforms respect Canadian privacy laws and are held accountable when

they fail to do so. However, Bill-C11 remains far from perfect, considering that it does not appear to cover political parties in any comprehensive way, it does not adequately limit the purposes for which an organization can use personal data, may create new complications in regard to personal consent despite the attempt to better define and protect consent, and may actually not clearly grant regulators such as the OPC with greater enforcement power with the introduction of the oversight Tribunal.

Recommendation 2 – Define Personal Privacy Clearly As a Human Right

A unique aspect of the EU GDPR, and the EU's more comprehensive protections of privacy across the board, is that the definition of privacy is grounded in the ideals of personal privacy as a human right on the part of data subjects. This is not included in Bill-C11, and accounts for a noticeable gap in the way that privacy and personal data are defined. Scassa (2020) notes that while privacy is a human right, as identified in international agreements that Canada is a part of, the Canadian government seems to be unwilling to fully commit to making that aspect a part of the proposed privacy legislation. Article 1 from the EU GDPR clearly states that "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (GDPR, 2018).

This continued resistance to defining privacy as the human right means that Recommendations 20, 22, and 24 from the ETHI Committee, which stated the need to bring Canadian legislation in line with the EU GDPR, have also not been addressed. The discrepancies between the recognition of privacy as a human right in the EU versus Canada have been identified by many, such as Houser and Voss (2018, 2019) and Wu (2018), and this was also a common thread through the ETHI Committee hearings, as

heard in the testimonies of Dunham, Therrien, Bennett, McEvoy, Stucke, and several others. In choosing to not consider this issue and to disregard the ETHI Committee recommendations, Bill-C11 may help to remedy some of the issues raised over the course of the Cambridge Analytica scandal, but it misses the mark in the areas just discussed.

5.3 Remaining Concerns: Where Regulation Requires Additional Attention

Canada has not addressed the structural aspects of media regulation. Nevertheless, the opportunity to enact stronger structural regulation remains important, as read in the recommendations from the BTLR and stronger structural regulations for social media platforms under the supervision of the Canadian Radio-television and Telecommunications Commission (CRTC) could be very helpful. Here I am informed by Wu's work on structural regulation in the US, where there is a history of strong anti-trust, recognizing that Canada does not have a similar tradition. The following recommendations will also consider the need for global collaboration between governments around the world to structurally regulate global social media companies.

Recommendation 3 – Break-ups or Structural Partitions

Ideally Canada would have just as much potential to push for the break-up of monopolistic social media platforms as does the US. However, considering the global nature of social media platforms like Facebook, one country alone cannot enforce such a measure, especially since most of the companies are not located in Canada. The US is the only country where such domestic regulation is considered effective, although even there, social media companies can offshore their data outside the US should they decide that they find regulation too restrictive. Instead of break-ups, in Canada, structurally partitioning platforms might be a more realistic proposition. For example, companies that

own two or more different platforms could be required to separate their different services, thus mitigating data flows between them. In Facebook's case, this would mean that it would no longer be allowed to share user data across its main Facebook service, and its secondary services such as Instagram and WhatsApp, among other, smaller services. Thus, each subsidiary company would be responsible for its own data and would not be able to share the data of its users for the purposes of marketing or advertisement. This sort of regulation was recently implemented with a certain level of success in Germany,[45] and it might be possible for Canada to work with other countries to harmonize this sort of regulation.

The function of this type of regulation is two-fold. First, it mitigates the huge amount of personal data that a single company alone can collect and use by creating walls between its various branches to limit the sharing of data between them. Second, break-ups promote competition within the newly segmented market and provide consumers with more choices and options about the services they have access to. Competition encourages companies to consider and respect consumer choice, wherein companies must vie for consumer attention, as they cannot rely on consumers having to agree to data policies or be excluded entirely. In this context, calls for better data protections from consumers are more likely to be heeded. Structural partitions can also help to ensure that

---

[45] Wherein the Government ruled that Facebook had to enact structural partitions between its different services, "Facebook would only be allowed to assign data from WhatsApp or Instagram to its main Facebook app accounts if users consented voluntarily. Collecting data from third-party websites and assigning it to Facebook would similarly require consent" (Busvine, 1, https://www.reuters.com/article/us-facebook-germany-idUSKCN1PW0SW). If such consent is withheld, then Facebook must restrict its collection and combination of data from the different services or will face heavy fines. The case summery of Germany's Federal Cartel Office decision can be found here; https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568

companies have less access to data, forcing a company not to link all a consumer's data across all their platforms, such as requiring WhatsApp to be self contained and not feed into marketing demographics for Facebook advertising. As Wu explains, "reintroducing competition into social media space… measured by matters like greater protection of privacy, could mean a lot to the public (Wu, 2018, p.133) And while structural partitions do not provide the same competitiveness between partitioned branches of the company as a full break up would, they nonetheless still encourage a certain level of diversity in services and make it easier for consumers to choose the service they want. For example, having Instagram without a Facebook profile and not having all their data available through Facebook resulting from cross-platform data collection. In short, "the simplest way to break the power of Facebook is breaking up Facebook" (Wu, 2018, p. 133).

Recommendation 4 – Market Concentration Levels

Building on the notion of break-ups or structural partitions, a set of regulations around market concentration levels could also help to ensure that no single company was cornering a particular media market, allowing them to set the rules for privacy and personal data regarding their services due to their sheer size and service provision monopolies. This sort of regulation would ensure that no single company is permitted to own more than a certain percentage of any given media sector before they are no longer allowed to merge with other companies in the same sector. Although, questions of how media markets are segmented complicates how much a company can own, as companies become more vertically integrated across different layers of the media markets.

Like the function of break-ups and structural partitions, the function of limiting market dominance through controlling concentration levels encourages stronger

competition and ensures that consumers have options if they are unhappy with a particular company's personal data protection and privacy policies. It also ensures that they are not forced to rely on a single company if they wish to access certain kinds of services, which would mean that they had to opt out of a service entirely if they did not agree with the company's data practices.

Recommendation 5 – Merger Reviews

When it comes to social media company mergers, market concentration and domination need to be key considerations within the process by which a company obtains regulator approval. Facebook should never have been allowed to acquire Instagram in the first place, considering that they did share the same market and the merger between them gave Facebook the opportunity to corner the market on posting platforms. The fact that they were able to go through with this merger without objection from regulators, both in the United States and the United Kingdom, is concerning. Therefore, the process for social media companies to acquire and merge with other companies needs to be much stricter, the process more rigorous, and one that includes stronger and more comprehensive merger reviews. Under the CRTC, the process for mergers should be a more involved process that requires companies to make a strong case for the merger before being allowed to do so, and the enforcement power given to regulators to deny mergers needs to be stronger, so that when a regulator blocks a merger on the grounds that the company is becoming to concentrated, the company must comply.

The function that this sort of regulation serves is to support the goals of market concentration regulation, as well as avoiding having to get to the stage where company break-ups are necessary. By having stricter measures on mergers, ideally, no company

would ever exceed the upper limit of market concentration and the result would keep the market unconcentrated enough for competition to thrive and consumer choice when it comes to privacy and data protections to be more comprehensive. As with the previous recommendations, Canadian regulators would likely be unable to enforce this solely on their own, considering that mergers happen on a global scale, well outside of the reach of Canadian regulators. However, for Canadian companies, or companies hoping to operate in the Canadian market, setting strong merger reviews is a step in the right direction.

5.4 Final Words

As it stands, there remains much work to be done regarding privacy and personal data protection in Canada. The Cambridge Analytica and Facebook scandal catalyzed discussion on the topic. Starting back in 2009, with the CIPPIC complaint to the OPC, and through the investigation and report by the ETHI Committee, as well as through the BTLR proceedings, this thesis has explored the different regulatory measures being proposed to improve personal data protection and privacy regulations in Canada, including behavioral and structural regulatory solutions that might mitigate similar scandals from occurring in the future. Social media and other data platform companies are massive and powerful, and while the introduction of Bill C-11 is going in the right direction, the Cambridge Analytica scandal demonstrated that there is much more at play than just the practices of social media platforms when it comes to privacy and personal data protection. A more comprehensive examination of the entirety of the global data ecosystem, including considering the roles of data brokers, internet companies outside of the social media archetype – such as Google – and marketing and advertising companies

in the collection, use and disclosure of personal data would be needed to properly understand how personal data are handled, not only in Canada, but around the world. Additionally, when investigating the types of regulation available to address concerns around the data practices of these sorts of entities, whether that regulation be structural, behavioural, or content focused, there needs to be an evaluation of regulation practices within nation states and across the world, to identify existing best practices, where there are robust standards, and to develop opportunities for cross jurisdictional collaboration. The research conducted in this thesis, in a small way contributes to this process.

APPENDIX 1

ETHI Committee Documents analyzed in the thesis.

House of Commons Committee on Access to Information, Privacy and Ethics (ETHI) (2018). *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data-opolies*. Ottawa: Government of Canada.

_and International Grand Committee (May 2019). Big Data, Privacy & Democracy. Ottawa: Government of Canada.

_42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-99/evidence

_42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-100/evidence

_42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-101/evidence

_42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-102/evidence

_42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-106/evidence

_42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-109/evidence

_42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-116/evidence

_42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-119/evidence

References

Babe, R., & Babe, R. E. (1990). Telecommunications in Canada. Retrieved from https://ebookcentral-proquest-com.proxy.library.carleton.ca

Bridy, A. (2018). Remediating Social Media: A Layer-Conscious Approach. BUJ Sci. & Tech. L., 24, 193. https://heinonline.org/HOL/Page?handle=hein.journals/jstl24&div=11&g_sent=1&casa_token=&collection=journals

Bogost, I., & Montfort, N. (2009). Platform studies: Frequently questioned answers. https://escholarship.org/uc/item/01r0k9br

Cadwalladr, C. (2017, May 07). The great British Brexit robbery: How our democracy was hijacked. Retrieved August 13, 2020, from https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Cannon, Robert (2003) "The Legacy of the Federal Communications Commission's Computer Inquiries," *Federal Communications Law Journal*: Vol. 55: Iss. 2, Article 2. Available at: http://www.repository.law.indiana.edu/fclj/vol55/iss2/2

Canada, Elizabeth Denham, Assistant Privacy Commissioner of Canada (July 16, 2009). *Report of the Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*.

Canada, Personal Information Protection and Electronic Documents Act (2000) 5c. https://www. priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Canada, Criminal Code (R.S.C., 1985, c. C-46)

Canada, Creative Canada Policy Framework (2017) https://www.canada.ca/content/dam/pch/ documents/campaigns/creative-canada/CCCadreFramework-EN.pdf

Canada, Charter of Rights and Freedoms, Constitution Act, 1982.

Canada, Privacy Act (1985). https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html

Canada, House of Commons Committee on Access to Information, Privacy and Ethics (ETHI) (2018). *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data-opolies*. Ottawa: Government of Canada.

Canada, House of Commons Committee on Access to Information, Privacy and Ethics (ETHI) and International Grand Committee (May 2019). Big Data, Privacy & Democracy. Ottawa: Government of Canada.

Canada, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-99/evidence

Canada, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-100/evidence

Canada, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-101/evidence

Canada, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-102/evidence

Canada, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-106/evidence

Canada, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-109/evidence

Canada, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-116/evidence

Canada, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 42nd Parliament, 1st Session (2018). Breach of personal information involving Cambridge Analytica and Facebook. Retrieved from ETHI Committee Meeting website: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-119/evidence

Canada, Parliament of Canada (2020). *Digital Charter Implementation Act, 2020*. Retrieved from The Parliament of Canada website: https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading#ID0E0ZB0BA

CIPPIC, (2006) On the Data Trail Report. https://cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf

CIPPIC, (2018) Back on the Data Trail Report. https://databrokers.cippic.ca/wp-content/uploads/2019/04/CIPPIC-Back_on_the_Data_Trail.pdf

Citron, D. K., & Wittes, B. (2017). The internet will not break: Denying bad Samaritans sec. 230 immunity. Fordham L. Rev., 86, 401. https://heinonline.org/HOL/Page?handle=hein.journals/flr86&div=19&g_sent=1&casa_token=&collection=journals

Davies, H. (2015, December 11). Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users. Retrieved August 13, 2020, from https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises. (2019, February 28). Retrieved August 13, 2020, from https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

Grassegger, H., & Krogerus, M. (2017, January 28). The Data That Turned the World Upside Down. Retrieved August 13, 2020, from https://publicpolicy.stanford.edu/news/data-turned-world-upside-down

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

Gillespie, T. (2010). *The politics of "platforms*". New Media and Society. SAGE.

Regulation (EU) 2016/679 General Data Protection Regulation (2018). *Official Journal of the European Union* L119, pp.1-88.

Kimberly A. Houser & W. Gregory Voss. (2019), *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*. Am Bus Law J, 56: 287-344. McChesney, R. W. (2013). *Digital disconnect: How capitalism is turning the Internet against democracy*. New Press, The.

Keller, D. (2018). Internet platforms: observations on speech, danger, and money. Hoover Institution's Aegis Paper Series, (1807). https://papers.ssrn.com/sol3/papers.cfm? abstract_id=3262936

Keller, D. (2019). Who Do You Sue? State and Platform Hybrid Power over Online Speech. Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1902. Available at https://www.lawfareblog.com/who-do-you-sue-state-and platform-hybrid-power-over-online-speech

Kimberly A. Houser & W. Gregory Voss. (2018). *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy*, 25 RICH. J.L. & TECH. 1, 58-70

Kimberly A. Houser & W. Gregory Voss, (2018). *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 1, 58-70

Kitchin, Rob. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. Sage Publications.

McChesney, R. W. (2013). *Digital disconnect: How capitalism is turning the Internet against democracy*. New Press, The.

Miglicco, Gary (2018). GDPR is here and it is time to get serious. Computer Fraud & Security Volume 2018, Issue 9, September 2018, Pages 9-12. https://doi.org/10.1016/S1361-3723(18)30085-Xdoi:10.1111/ablj.12139

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein .journals/washlr79&div=16&id=&page=

Oeldorf-Hirsch, Anne. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, communication and society.* 23.1 (2020): 128–147. Web.

Olson, P. (2014, October 6). Facebook Closes $19 Billion WhatsApp Deal. Retrieved from https://www.forbes.com/sites/parmyolson/2014/10/06/facebook-closes-19-billion-whatsapp-deal/#5f1af2d45c66

Pal, Leslie A., and Judith Maxwell (January 2004). Assessing the Public Interest in the 21st Century: A Framework. Paper prepared for the External Advisory Committee on Smart Regulation, Chaired by GaétanLussier. Canadian Policy Research Networks. Retrieved August 2015

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump Consultants Exploited the Facebook Data of Millions. Retrieved from https://www.nytimes .com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Rusil, E. (2012, April 9). Facebook Buys Instagram for $1 Billion. Retrieved from https://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/

Scassa, T. (2020, December 12). *The Gutting of Consent in Bill C-11*. Teresa Scassa – Blog.http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=336%3Athe-gutting-of-consent-in-bill-c-11&Itemid=80.

Scassa, T. (2021, January 12). *Data Mobility (Portability) in Canada's Bill C-11*. Teresa Scassa – Blog. http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=338%3Adata-mobility-portability-in-canadas-bill-c-11&Itemid=80.

Scassa, T. (2021, January 4). *How do new data protection enforcement provisions in Canada's Bill C-11 measure up?* Teresa Scassa - Blog. http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=337%3Ahow-do-new-data-protection-enforcement-provisions-in-canadas-bill-c-11-measure-up%3F&Itemid=80.

Scassa, T. (2020, December 6). *Data for Good?: An Assessment of the Proposed Exception in Canada's Private Sector Data Protection Law Reform Bill*. Teresa Scassa - Blog. http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=335%3Adata-for-good%3F-an-assessment-of-the-proposed-exception-in-canada%E2%80%99s-private-sector-data-protection-law-reform-bill&Itemid=80.

Schwartz, M. (2017, March 30). Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate. Retrieved August 13, 2020, from https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/

Srinivasan, D. (2019). The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy. *Berkeley Business Law Journal*, *16*(1), 1–39. https://lawcat.berkeley.edu/record/1128876?ln=en.

United Kingdom (2019). *Unlocking digital competition, Report of the Digital Competition Expert Panel*. London, UK: Author.

Vaidyanathan, S. (2018). *Antisocial media: How Facebook disconnects us and undermines democracy*. Oxford University Press.

Vincent, J. (2019, February 7). Facebook ordered to stop combining WhatsApp and Instagram data without consent in Germany. Retrieved September 30, 2019, from https://www.theverge.com/2019/2/7/18215143/facebook-whatsapp-instagram-third-party-user-data-combined-banned-germany-fco-competition.

Winseck, D. (2018). Growth of the Network Media Economy in Canada, 1984-2017. Canadian Media Concentration Research Project (CMCRP). doi:10.22215/cmcrp/2018.1

Winseck, D. (2019). Growth of the Network Media Economy in Canada, 1984-2018. Canadian Media Concentration Research Project (CMCRP).

Winseck, D. (2020). Growth of the Network Media Economy in Canada, 1984-2019. Canadian Media Concentration Research Project (CMCRP).

Winseck, D. (2020).' Vampire Squids, 'the Broken Internet' and Platform Regulation', Journal of Digital Media & Policy, 11:X, pp. X-Y

Wu, T. (2003). Network neutrality, broadband discrimination. J. on Telecomm. & High Tech. L., 2, 141.

Wu, T. (2010). The master switch: The rise and fall of information empires. Vintage.

Wu, T. (2018). The curse of bigness: Antitrust in the new gilded age. Random House Audio.