Defining Privacy:
A critical investigation of Canadian political discourse

by

Sandra Schwab

A thesis submitted in partial fulfillment of the requirements for the degrees of

Master of Arts in Humanities Computing

&

Master of Library and Information Studies

Humanities Computing / Library and Information Studies

University of Alberta

Abstract

Canada's federal privacy legislation does not include a definition or explanation of the word 'privacy', yet an understanding of the meaning of 'privacy' is essential to understanding how much or how little privacy to expect in terms of the protections afforded within the law. The purpose of this thesis is to uncover the definition of 'privacy' in the House of Commons as it is used by Members of Parliament (MPs) by examining the language and context within which the word is used.

To prepare for the text analysis, a comprehensive literature review was conducted, summarizing the two key pieces of federal privacy legislation in Canada: the Privacy Act and the Personal Information Protection and Electronic Documents Act. This review also investigated other related pieces of legislation, government documents, and jurisprudence on the topic of federal privacy protection in Canada.

The text analysis was conducted using the XML transcripts of the House of Commons Debates, commonly known as Hansard, spanning a ten-year period that included all of the proceedings from the 39th to the 41st Parliaments. This period, between 2006 and 2015 inclusive, consisted of the entirety of Right Honourable Stephen Harper's Conservative Party of Canada governance in the House of Commons.

The first stage of text analysis used natural language processing modules in Python to generate frequency counts and concordances with a focus on the word 'privacy'. Between 2006 and 2015, there was an observable overall increase in the frequency of the word 'privacy'. The analysis of the concordance data uncovered that 'privacy' was commonly used in the phrase 'privacy rights', and a further frequency analysis on this phrase uncovered that it was most frequently used in 2014. Another finding from the concordance data was the occurrence of the qualifying phrase 'law-abiding Canadians', accompanying both 'privacy' and 'privacy rights'. These two trends--the high frequency of the phrase 'privacy rights' in 2014, and the occurrence of the phrase 'law-abiding Canadians'--formed the basis for the second stage of the text analysis, a Critical Discourse Analysis of a debate that occurred on May 5, 2014.

This specific transcript was selected because it had the highest frequency of the phrase 'privacy rights' compared to all the other Sittings in 2014. Through the Critical Discourse

Analysis of the debate, based on the methodology of Fairclough, it was determined that MPs do not have a clear understanding of the two core pieces of federal privacy legislation in Canada, nor do they comprehend the relationship between 'privacy' and the Canadian Charter of Rights and Freedoms. This was evinced by multiple unrefuted references to a 'Charter right to privacy', which is a false characterization of the Charter, as well as a fundamental misunderstanding of what comprises 'personal information' in Canadian privacy law, something that is clearly defined in the Privacy Act. Furthermore, the repeated reference to the 'privacy rights of law-abiding Canadians' uncovered a strong ideological bias among all MPs that narrowly defines privacy as secrecy, preferencing the protection of privacy afforded to Canadians who abide by the law and marginalizing the protection of privacy afforded to those who don't.

According to Westin, a broader conceptualization of privacy as anonymity rather than secrecy allows individuals to freely express their thoughts, viewpoints, and political beliefs, without the fear of ridicule, alienation, or punishment (33-34). The narrow definition of privacy held by MPs as a 'right to secrecy for Canadians who abide by the law' can have what Solove describes as a 'chilling effect' on society as a whole, within which the perceived lack of anonymity has the result of suppressing the autonomy and creativity of all individuals (765).

Acknowledgments

I would first like to thank my thesis supervisors: Dr. Geoffrey Rockwell of Humanities Computing in the Faculty of Arts at the University of Alberta; and Dr. Michael McNally of the School of Library and Information Studies at the University of Alberta.

I would also like to thank the members of my examining committee: Dr. Harvey Quamen of Humanities Computing in the Faculty of Arts at the University of Alberta; and Dr. Tami Oliphant of the School of Library and Information Studies at the University of Alberta.

I wish to express my gratitude to the donors of the J Gordin Kaplan Graduate Student Award and the Michael Silver Memorial Travel Award in Library and Information Studies. Both awards made it possible for me to present my thesis research at the international conference for the International Association for Social Science Information Services & Technology (IASSIST), in Bergen, Norway.

I am also grateful for the generous assistance of Hedmark University College and Dr. Hans Kristian Rustad of the Department of Humanities at Hedmark University College for sponsoring my three month student exchange in Hamar, Norway; the place where I began to write my thesis in earnest.

I would also like to express my gratitude for the support, guidance, and mentorship of those who supervised my employment at the University of Alberta: Dr. Sean Gouglas of Humanities Computing, who gave me a lot of good advice and was the source of many passable puns; and the librarian Anna Bombak along with the rest of the Digital Initiatives unit in the University of Alberta Libraries, who welcomed me into the wonderful world of Data Librarianship.

Finally, I am grateful for the support of my husband, the love of my life, and my friends and family.

Table of Contents

List of Tables

List of Figures

1 Introduction

Privacy is difficult to define. It encompasses the personal, social, technological, and legal domains of society in ways that overlap and diverge. Traditionally, privacy has been articulated as an issue of protecting one's personal space from intrusion, but with the rapid increase and ubiquity of information technology, the distinction between personal and public space is no longer easily identified.

The protection of privacy in Canada is regulated by laws at both levels of provincial and federal government. The majority of these laws are concerned with the privacy of personal information, in terms of how it is collected, used, stored, shared, and destroyed. Yet, in the case of federal privacy legislation, an actual definition of privacy has not been written in to the law.

Without an understanding of what privacy means, at least in terms of the two core federal privacy statutes, it is hard to manage expectations regarding when, where, and how much privacy will be afforded under Canadian law. By examining federal privacy legislation and the transcripts of political debates, this thesis will endeavour to construct a definition of privacy as it is commonly used by those who are responsible for the creation and enactment of privacy legislation, the politicians themselves.

This will involve a two-stage text analysis of the transcripts of the political debates that occurred in the House of Commons, commonly known as Hansard, between the years 2006 and 2015. The first stage will use computerized techniques to discover trends and patterns in word use over the ten-year period under investigation. The second stage will build on the first, with a focused critical analysis of the discourse of a single debate, which will be identified based on the results from the first stage of analysis.

Both stages of analysis will be supported by a comprehensive review of privacy legislation in Canada, including the historical basis for the enactment of the laws, and the legal literature produced as a result of their enforcement. These analyses will result in a clarification of the meaning of privacy as it is used by those who have the power to determine how much, or how little the privacy of Canadians is protected by the law.

In order to understand what privacy means to federal politicians in the context of their work, the system of politics in Canada must first be understood. The following section is a brief introduction to Canadian federal politics in terms of how it is organized and structured to support the creation and enactment of legislation.

The Canadian System of Government

The entirety of this section is described in terms of the Parliamentary publication *House of Commons Procedure and Practice*, 2nd Edition, edited by Audrey O'Brien and Marc Bosc. This publication includes information about precedents current to 2009, the midway point of the period under study. While Parliamentary procedures can and do change, the information provided here applies to the entirety of the study, unless otherwise noted.

Canada is a parliamentary democracy, which is a system of government that holds that the law is the supreme authority (O'Brian and Bosc). The law is communicated through carefully worded documents known as legislation, which serves the purpose of regulating what may or may not be done in Canada (O'Brian and Bosc). The power to create legislation resides in the Legislature, which includes the House of Commons and the Senate, and the Crown, which is represented by the Governor General (O'Brian and Bosc).

The 'Crown' is the term used in Canada to describe the state, which is the country's supreme authority (O'Brian and Bosc). This term is a recognition of the British Monarch, who is the formal head of state in Canada (O'Brian and Bosc). The Crown is represented by the Governor General, who is elected by the Queen on the advice of the Prime Minister of Canada. While the role of the Governor General is seen to be mostly symbolic, the Crown retains the "right to be consulted, to encourage and to warn" (O'Brian and Bosc). The primary responsibility of the Governor General in terms of legislative power is the granting or withholding of Royal Assent, which is required before a Bill can become a statute that determines the law (O'Brian and Bosc).

The Legislature consists of the Senate, also called the Upper House, and the House of Commons, which both have equal status in terms of privilege and power (O'Brian and Bosc). Senators are appointed by the Governor General, on the recommendation of the Prime Minister (O'Brian and Bosc). The House of Commons consists of elected Members of Parliament (MPs) (O'Brian and Bosc). Both the Senate and the House have a fixed number of seats based on the distribution of the population in the provinces and territories (O'Brian and Bosc). These numbers are periodically adjusted to reflect changes in the population (O'Brian and Bosc).

Both the Senate and the House of Commons must adopt the same legislation before it can be granted Royal Assent, and legislation can be introduced in either place (O'Brian and Bosc). The seating arrangement in both Houses is organized in terms of political party membership, where the Members affiliated with the governing political party sit to the right of the Speaker of the House, while the other Members sit to the left (O'Brian and Bosc). Political parties are distinguished in terms of their ideology, which involves the system of values that underlies the belief in how Canada ought to be governed (Dijk, "Political Discourse Analysis" 17; Fairclough, *Language and Power* 32; O'Brian and Bosc).

In the House of Commons, the political party with the highest number of elected MPs forms what is referred to as the government, while the MPs from the other parties are called the opposition, the largest of which is called the Official Opposition (O'Brian and Bosc). The Prime Minister, who is the leader of the governing party, along with the Cabinet, consisting of select members of the government, has the additional power of enacting government policies and programs, so long as they are accountable to and retain the confidence of the entire House of Commons (O'Brian and Bosc).

Elections determine what can be called the 'lifecycle of Parliament' (O'Brian and Bosc). In this sense, the term 'Parliament' refers both to the institution itself (made up of the Crown, Senate, and House of Commons) and the period of time within which the institution exercises

its powers (O'Brian and Bosc). A Parliament is dissolved when the Governor General calls an election, beginning again when the new Parliament is formed as a result of an election (O'Brian and Bosc). The House of Commons has a constitutionally-determined lifespan of five years, though elections can occur at any time within that period (O'Brian and Bosc). Legislation was introduced by the government in 2007 mandating that a fixed-date general election must occur every four years, on the third Monday in October (Library of Parliament, "Fixed-date Elections"). The first of these fixed-date elections occurred in 2015 (Library of Parliament, "Fixed-date Elections").

Parliaments are divided into time periods known as Sessions, which consist of a variable number of different sittings (O'Brian and Bosc). Sessions begin with a Speech from the Throne and end when Parliament is prorogued or dissolved (O'Brian and Bosc). While prorogation is only the end of a Session, and not a Parliament, it signals the end of all proceedings before Parliament, meaning that any 'unfinished business' is effectively dead, and must be reintroduced as if it had never existed when the new session starts (O'Brian and Bosc). This applies to Bills that have not yet received Royal Assent, although this has occasionally been overruled in the case of unanimous consent among the members of the House (O'Brian and Bosc).

A 'sitting' is a meeting of the House of Commons that occurs when Parliament is in session (O'Brian and Bosc). It follows a structured program consisting of a recurring sequence of business, including daily and routine proceedings, government orders, Bills from Private Members', and adjournment proceedings (O'Brian and Bosc). The entirety of this program is published in a number of different publications, depending on content (O'Brian and Bosc). One of these publications is the House of Commons Debates, otherwise known as Hansard, which is the transcribed, edited, and corrected record of what is said in the House (O'Brian and Bosc). The proceedings of the Senate are also published as Hansard, but in terms of this research, the use of the term Hansard will refer exclusively to the House of Commons.

The collection of texts selected for analysis in this thesis spans the entirety of the 39th to the 41st Parliaments, which cover a ten year period between 2006 and 2015. This collection comprises the entirety of The Right Honourable Stephen Harper's Conservative government in the House of Commons. While the 41st Parliament was a period of majority governance for the Conservative Party of Canada, the 39th and the 40th were both periods of minority governance (O'Brian and Bosc). A minority government occurs when a political party wins the most seats in the election, but not enough seats to hold a majority in the House of Commons, which during the time covered by this study, was 308 seats (Library of Parliament, "Parliaments"). The legislative power of the governing party is concentrated in the ability of Members to vote for or against proposed legislation, which means that a minority government has less of an influence on the outcomes of votes, and the subsequent legislative process of turning Bills into statutes (O'Brian and Bosc).

In terms of the House of Commons, the examination and enactment of legislation comprises a significant amount of the time spent in Parliament (O'Brian and Bosc). In order for a Bill to become a law it must first pass through a long procedural chain of standardized

motions; in fact, the debate and resulting decisions about bills in the House of Commons are not actually about the Bills themselves, rather, they are focused on the motions required to accompany them (O'Brian and Bosc). Though there can be differences in procedure and ordering, all Bills pass through the same stages, which include the following: a first reading; a second reading, involving a debatable motion and vote; a committee stage, which happens outside of the House; a report stage, where the report from the committee is presented to the House and debated; and finally, a third reading involving another debatable motion and vote (O'Brian and Bosc). Once a Bill passes through these stages, it is referred to the Senate, and then to the Governor General for Royal Assent (O'Brian and Bosc).

This process is what makes the transcripts of Hansard such a compelling resource. The interpretation of the meaning and intent of statutes can be aided in part by what Canadian legal scholar Ruth Sullivan describes as "extrinsic materials", which includes Hansard (659). She argues that the extensive discussion and debate by MPs of issues before the House provides strong evidence for understanding the underlying intent of the decisions that are ultimately made (659). In the case of this investigation, this means that the ways in which MPs discuss and debate privacy will provide persuasive evidence for determining what privacy actually means in the context of the House of Commons, and in the privacy legislation itself.

Purpose, Objectives, and Research Questions

The purpose of this research is to determine the meaning of privacy as it was used by the Members of the House of Commons between the 39th and 41st Parliaments.

Three interrelated objectives will serve this purpose. The first objective will be to understand what privacy has historically meant in Canada by conducting a review of the legislation, standing committee reports, and jurisprudence that pertain to Canadian privacy issues, as well as a review of the literature that contributed to the creation of these documents.

The second objective will measure the occurrence of the word 'privacy' within the context of its use in the House of Commons. This first stage of text analysis will ask the following questions: how many times does the word 'privacy' appear in the transcripts of Hansard, and is there an observable change in the frequency of use over the period under observation? Also, are there observable patterns of language use when 'privacy' is viewed in the context of the sentence within which it appears, and do these patterns change over time?

The third objective of this research will explain the trends regarding the frequency and contextual patterns observed in the first stage of analysis by asking the following question: why do Members of Parliament use the word 'privacy' in the way in which it has been observed, and how does the language used in the House of Commons contribute to an overall understanding of the meaning of the word?

These objectives and research questions will help to answer the primary research question underlying the purpose of this thesis: what is the meaning of privacy in the House of Commons as it was recorded in Hansard between the 39th to the 41st Parliaments?

The linguist Michael Stubbs argues that our understanding of language is mediated by a cultural understanding of how combinations of words can be combined to create meaning (*Words and Phrases* 3). The outcome of the textual analysis of Hansard will be more than just a list of words related to privacy and the number of times they were used; it will provide a deeper rationale for the meaning of privacy as it is used in the context of the House of Commons, which includes the beliefs, expectations, and evaluations of the MPs themselves (Stubbs, *Words and Phrases* 6).

The power in a parliamentary democracy such as Canada is expressed through the rule of law, which is carried out through the enactment of legislation that determines what can and can't be done in society. Privacy legislation in Canada generally determines what can and can't be done with regard to the personal information of citizens. In order to understand the law, we must understand its intent, and in the case of privacy law, this requires an understanding of the meaning of privacy itself. While none of the federal privacy legislation contains a definition of the word privacy, its meaning can be ascertained through an examination of language and context within which it is used.

Methods of Analysis

The two stages of analysis that will comprise the bulk of the research in this thesis will consist of two different but complementary approaches to the study of language in use. The first stage will involve the computerized processing of the entire body of text, while the second stage will involve a critical investigation of a specific parliamentary debate, selected based on the trends identified in the initial text analysis.

Computerized Text Analysis

Hansard is a very large body of text. Between 2006 and 2014, almost 69 million words were spoken and transcribed. The entirety of this text will be analyzed using natural language processing techniques in the Python coding language in order to collect data about patterns related to the use of the word 'privacy', as well as the phrases and sentences in which it appears. The purpose of this first stage of analysis is to uncover trends in word use over time, as well as to determine what other types of words are used in conjunction with 'privacy'.

Critical Discourse Analysis

The findings from the text analysis research will be used to inform the next stage of the research, which will consist of a Critical Discourse Analysis of specific trends in language use found in Hansard. While computerized text analysis is a form of "distant reading", a term coined by Franco Moretti that refers to analyzing a text "from a distance" ("Conjectures on World Literature", 57), Critical Discourse Analysis requires conducting a "close reading" of a text as a means of uncovering the ways in which language can be used as tool of social power and dominance in society (Taylor 5; Van Dijk "Critical Discourse Analysis", 352).

Through a distant and deep textual analysis of the transcripts of Hansard, this thesis will endeavour to construct a meaningful definition of privacy as it is used by the MPs who represent the citizens of Canada in the House of Commons. Privacy can no longer be conceptualized as an issue of distinguishing the difference between what is public and what is private space.

Information technology has evolved in such a way that makes this distinction meaningless. The structure of the internet lends itself to a landscape that includes pockets of digital private spaces enclosed within very large and penetrable public spaces; an example of this is online banking, which involves the access of highly secure information via mobile devices on public wi-fi networks. Mobile devices themselves leave a trail of data behind them, which includes not only the location of the device, but what kinds of things it has been used for; this includes the contents of text messages and emails, web browsing histories, and in some cases, physiological data such as heart rate.

The unintended disclosure or consolidation of this personal data can lead to a range of harmful consequences for individuals, such as identity theft or fraud. But it is the awareness of these consequences that lead individuals to make decisions that affect society as a whole. The knowledge that one's digital life is not secure contributes to what Canadian legal scholar Daniel Solove describes as a 'chilling effect' on society (765), regardless of whether the privacy issue involves overt breaches of personal information or more passive methods of surveillance like security cameras. This 'chilling effect' is harmful because it narrows the free expression of individuals in society, which runs counter to the normative ideals of the parliamentary democracy within which Canadians are governed.

By determining the meaning of privacy as it is understood by MPs, we can better understand the intent of the legislation in terms of when, where, and how the protection of privacy can be expected in Canada. This knowledge can empower citizens to speak up when their expectations of privacy are not met, or when they are blatantly disregarded.

Structure of this Thesis

This thesis is arranged as a series of chapters that focus on the distinct stages of this research. This chapter has provided the introductory context in terms of the purpose of the entire thesis, which is an investigation of the discourse of privacy in the House of Commons as a means of constructing a definition of privacy that can inform the privacy expectations of Canadian citizens. Chapter 2 will contain a comprehensive review of federal privacy legislation in Canada, including its history and the jurisprudence that relates to its enforcement. Chapter 3 will include the first stage of the text analysis, which will involve a complete methodological description as well as the results from the analysis itself. Chapter 4 will focus on the second stage of the text analysis, which will include a comprehensive explanation of the methodology of Critical Discourse Analysis embedded with the actual analysis of a text. Chapter 5 will conclude the thesis, discussing the overall results, the limitations of the research, and areas of interest for further study.

2 Privacy

Privacy is a uniquely personal, social, technological, and legal issue. The personal aspect of privacy concerns what some consider to be a "right to be left alone", whether that means solitude behind the walls of one's own home, or the ability to be anonymous in public spaces. Socially, privacy is the ability for an individual to maintain control over their personal information while simultaneously contributing to the increasing information needs of society. This issue has been characterized as a balance between the competing needs of confidentiality and access to information. Technologically, the idea of privacy continues to evolve, as individuals become more willing to trade a greater amount of personal information for access to goods, services, and social networks. Yet the use, disclosure, and ownership of that information by government and business is increasingly unclear, especially when seemingly disparate pieces of information can be linked in such a way that individuals can become identifiable. Privacy law is important when harms occur from privacy violations, yet none of the Canadian legislation responsible for the protection of privacy provide a definition or explanation of what privacy actually means.

Shelia Finestone, a former Member of Parliament and Senator, wrote the following description of privacy in a report to the Standing Committee on Human Rights and the Status of Persons with Disabilities. Her characterization of the complexity of the issue perfectly covers the topics that will be investigated in this chapter.

> To experts, privacy is the right to enjoy private space, to conduct private communications, to be free from surveillance and to respect the sanctity of one's body. To the average Canadian, privacy is a question of power -- the ability to control one's personal information and to remain anonymous by choice (Finestone v).

Purpose of this Chapter

The purpose of this chapter is to uncover what privacy has historically meant in Canada, and more specifically, within the domain of Canadian federal politics. The boundaries of this investigation will primarily include references to Canadian legislation and scholarship, though concepts from seminal literature in the philosophy of privacy will be included as a means of guiding and framing the review.

Reports to Standing Committees, such as the source from the quote above, can provide valuable insight into the spirit and meaning of legislation, helping to clarify core concepts and guiding principles in ways the wording of the legislation cannot. These reports are included in Sullivan's concept of "extrinsic materials" (659), and they consist of non-partisan and carefully reasoned conclusions regarding issues under legislative review (684). In some cases, these reports play a major role in the crafting of legislation before it is passed (Sullivan 684), while in others, they constitute the legislated mandatory review of a law after a specific time has passed.

On the other hand, jurisprudence and judgments from court cases involve the legal interpretation of legislation, which helps to clarify the real-world context of the law and its effect

on Canadians. This chapter will examine key court cases involving federal privacy legislation in an attempt to understand the meaning of privacy, both in support of and as a result of the Canadian privacy legislation that has been created with the intention of privacy protection.

Overview of this Chapter

This chapter will begin with Section 2.1, which includes a description of the federal legislation in Canada that regulates the issue of privacy, as well as international agreements to which Canada is a member. This includes the Canadian Charter of Rights and Freedoms, the Privacy Act, the Personal Information and Protection of Electronic Documents Act (PIPEDA), as well as brief descriptions of the Criminal Code and the Telecommunications Act. International agreements including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Organisation for Economic Co-operation and Development guidelines concerning privacy and transborder data flows will also be discussed, as they have all influenced Canadian privacy legislation in some way.

Section 2.2 will uncover the definitions and taxonomies of privacy that have informed and influenced Canadian jurisprudence. The courts are responsible for interpreting Canadian legislation, and their subsequent rulings often bring more meaning to the laws than the wording of the laws themselves. Especially important in this section is a discussion of what it means to have a 'reasonable expectation of privacy'. This phrase appears over and over in both the legislation and the courts, yet without an understanding of the meaning of privacy, it is hard to know how and when to reasonably expect it.

Section 2.3 will discuss the function of privacy for individuals and for society as a whole. A common argument in defence of less privacy, the 'nothing to hide' argument, will be discussed and contrasted with the understanding of privacy developed in the chapter. Finally, the section and chapter will conclude with a review of the concept of privacy as power.

2.1 Privacy Legislation in Canada

Canadian privacy protection has been described by Finestone as a patchwork garden full of weeds (26). This description comes from a 1997 report by the Standing Committee on Human Rights and the Status of Persons with Disabilities that investigated the past and future of privacy legislation in Canada. Her rationale for the statement still rings true in the almost 20 years that have passed since the report was published. Canada's federal nature, with divisions of power and responsibility split between the provincial and federal governments, has led to a patchwork of privacy protection that suffers from a lack of enforcement and scope (25-26). At the time the report was written, the only specific federal privacy legislation in Canada was the Privacy Act. This legislation, still in force today, only protects the privacy of personal information held by federal government departments and agencies. Privacy laws concerned with personal information held by non-government organizations, namely businesses, currently exist, but the patchwork metaphor still applies.

This section will examine and describe Canadian federal privacy legislation, specifically the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). While some provinces have their own privacy laws, those documents are beyond the scope of this investigation. This section will also briefly cover international agreements to which Canada is a signee, as well as the Canadian Charter of Rights and Freedoms.

International Agreements

Universal Declaration of Human Rights (UDHR)

In 1948 the Universal Declaration of Human Rights (UDHR) was adopted by the United Nations General Assembly. The aftermath of WWII brought human rights to the forefront of issues important to all societies at an international scale (Finestone 23, Schabas 407). Article 12 of the Declaration states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation" and that "everyone has the right to the protection of the law against such interference or attacks". The UDHR clearly establishes privacy as a fundamental right for all people.

International Covenant on Civil and Political Rights (ICCPR)

In 1976 Canada acceded to the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the Covenant, adopted by the United Nations General Assembly in 1966, has a provision identical to Article 12 of the UDHR mandating the right to privacy and freedom from unlawful interference and attacks. These documents, specifically UDHR, were instrumental in guiding the creation of the Canadian Charter of Rights and Freedoms (Schabas 405).

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

In 1980, the Organisation for Economic Co-operation and Development (OECD) released a set of guidelines for the protection of privacy and transborder flows of personal data (McIsaac, Shields, and Klein 5.1.1). Their objective was to "ensure that all international data flows were not completely blocked by protective measures taken nationally....and to harmonise the data protection practices of member countries by establishing some minimum standards for handling personal information" (Finestone 26). Twenty-three countries joined with Canada to

adhere to the guidelines, passing information privacy laws in accordance with the principles. Both the Privacy Act and PIPEDA were influenced by this adherence (Finestone 26; McIsaac, Shields, and Klein 1.3.3). The countries that have agreed to enact the OECD principles are known as 'Member countries'.

The guidelines themselves are voluntary, and consist of basic principles that apply to the protection of personal information at both the national and international level. The nationally applicable principles are: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability (McIsaac, Shields, and Klein 5.1.1). The guidelines refer to the individual or organization collecting the data as the 'data collector', while the individual whose personal information is being collected is called the 'data subject'.

Collection limitation means that the collection of personal data should be subject to limits and collected in a lawful and fair manner with the consent of the data subject (*OECD Guidelines* 14). Data quality refers to the relevance and accuracy of the data collection, meaning that only data specific to the purpose of use should be collected, and that it should be kept up-to-date (15). Purpose specification means that the purpose of the data collection should be understood by the data collector and the data subject at the time of collection, and that the subsequent use of the data be limited to that initial purpose (15). Use limitation means that the data should not be disclosed or made available for purposes other than the initial reason for collection, unless the data subject has consented, or under the authority of the law (15). Security safeguards imply that data should be reasonably protected against loss, unauthorized access, destruction, use, disclosure, or modification (15). Openness refers to the practice of making the practices and policies of data protection legislation or laws publicly available, as well as the ability to establish the existence, nature, and purpose of the data being collected (15). Individual participation concerns data subjects and their ability to confirm the existence of their own personal data, as well as the means to access and control that data (16). Finally, accountability refers to the data controller, and their responsibility to comply with the above principles (16).

The international principles are focused on co-operation between nations regarding transborder exchanges of data, including that Member countries consider the national and international implications for data processing and export; ensuring that data can flow in a secure and uninterrupted manner between Member countries; that Member countries ensure that data flows are unrestricted when regulated appropriately; and, that Member countries refrain from passing legislation that create unnecessary obstacles to data flow (*OECD Guidelines* 16-17; McIsaac, Shields, and Klein 5.1.1).

These principles, specifically the ones that apply at the national level, have been influential in the design of public and private sector privacy legislation in Canada, as evinced by the language present in both pieces of legislation. The descriptions of the general principles of the OECD guidelines are instructive of the meanings in the related sections of both the Privacy Act and PIPEDA.

Canadian Legislation

Canadian Charter of Rights and Freedoms

In 1982 the Canadian Charter of Rights and Freedoms came into force as Part I of the Constitution Act, which itself was enacted as Schedule B to the Canada Act, 1982 (note 80 at page 53). The Charter does not specifically include privacy as a right. Despite this, the courts in Canada have consistently interpreted Sections 7 and 8 as guarding against unreasonable privacy invasions (Finestone 24). Section 7 provides for the "right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice" and s. 8 states that "everyone has the right to be secure against unreasonable search or seizure".

Section 8 is listed as the second of eight legal rights in the Charter, and while it is not specifically framed as being 'free' from something, it has been interpreted by the courts as a 'right to be free' from unreasonable search and seizure (Bailey 284). The term 'unreasonable' is important here, as the courts must decide where the line between a reasonable search and an unreasonable search lies (Bailey 284). In order for a citizen to understand their rights within the Charter, they need to have an understanding of what reasonable means, so that they can have a reasonable expectation of how to behave according to the law.

The idea of 'reasonable expectations', especially in terms of privacy, will be addressed in the next section of this chapter. The discussion will be framed in the context of a landmark Supreme Court ruling on privacy invoking s. 8 of the Charter.

Proposals were made to include privacy as a constitutional right before the Charter even became law. In 1979, the federal government itself considered adding a formal clause to the Charter, and in 1981 the Canadian Bar Association advocated strongly for the inclusion of privacy provisions (Finestone 25). Even if privacy had been enshrined as a constitutional right, Finestone argues that there would still be limitations in the scope of the protection (25). Section 1 of the Charter allows for reasonable limits on any Charter right if those limits are "prescribed by law as can be demonstrably justified in a free and democratic society". Furthermore, the Charter itself only applies to the laws and activities of government and not the private sector (Finestone 25).

The Privacy Act

Canada's first overarching privacy legislation came into force in 1983 as the Privacy Act. The legislation is a means of regulating the collection (s. 4), use (s. 5(1)), disclosure (s. 5(2)), and disposal (s.6(3)) of personal information held by the federal government. It covers all federal government departments and most federal agencies (s. 3(a,b) 'personal information'), but not all Crown corporations or the federally regulated private sector (Schedule s. 3). It requires each government institution, with exceptions, to record the nature and extent of personal information it controls in a central index to which everyone has reasonable access (s. 11).

The Privacy Act is essentially a piece of legislation that mandates the protection of data (Finestone 26; Thacker 4). Its purpose is to enable individuals to have control over the

personal information they exchange to receive government benefits without being subject to an uncontrolled and unaccountable bureaucracy (Thacker 4-5).

Personal information, according to the Privacy Act, means "information about an identifiable individual that is recorded in any form" (s. 3) including race, national or ethnic origin, colour, religion, age or marital status (a); education, medical, financial, criminal or employment history (b); identifying numbers or symbols (c); address, fingerprints or blood type (d); personal opinions or views, with exceptions (e); private correspondence with the government (f); the views or opinions of others about an identifiable individual, with exceptions (g, h); and the name of an individual, if disclosure of the name would reveal other information (i). It's important to note that this is a non-restrictive list of illustrative examples of personal information (McIsaac, Shields, and Klein 3.1.2).

There are three distinct bodies responsible for upholding and maintaining different aspects of the Privacy Act. The Privacy Commissioner receives complaints and investigates non-compliance (Privacy Act, s. 29(1)), the Treasury Board Secretariat co-ordinates and implements the Act (Finestone 26), and the Department of Justice is responsible for the policy implications that arise as a result of the Act (Finestone 26). The designated head of the government department the Act applies to is responsible for compliance, and each government institution must designate a Privacy Coordinator that receives and processes access requests (Thacker 4).

The enforcement powers of the Privacy Commissioner in terms of the Privacy Act apply to requests for personal information and breaches of information privacy (s. 29(1)). When a breach of the Act occurs, the Privacy Commissioner is responsible for an investigation, and in some cases the production of a report with recommendations (Privacy Act, s. 35(2)). The information access aspect of the Privacy Act stems from the fact that the Access to Information Act was enacted at the same time as the Privacy Act (Finestone 26). The interplay of these two Acts results, according to Finestone, is to ensure a balance of privacy and access, where information held by government institutions is kept private if its personal and kept publicly available if its non-personal (26).

Section 75(2) required a comprehensive review of the provisions and operations of the Privacy Act by July 1, 1986, three years after the Act came into force (Thacker 1). An identical provision was included in the Access to Information Act (Thacker 1). The review and resulting report, titled *Open and Shut: Enhancing the Right to Know and the Right to Privacy,* was undertaken by the Standing Committee on Justice and Solicitor General and released in 1987.

The report made a number of recommendations for the amendment of the Privacy Act, notably, that the definition of personal information to be broadened (Thacker 24, 58, 72); that the audit and enforcement powers of the Privacy Commissioner be extended (Thacker 38); and, that a definition of privacy be explicitly included in the Act (Thacker 38). The recommended definition of privacy is the following: "(p)rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is to be communicated to others" (Thacker 58).

An actual definition of privacy is absent from any of the Canadian legislation on privacy, and despite the recommendation for its inclusion in the Privacy Act in 1987, it has yet to appear there, or anywhere. In fact, not one of the recommendations made in the 1987 report were ever enacted ("Letter to the Standing Committee"). The definition suggested by the report is focused on describing the meaning of privacy as a concept related to personal information, rather than attempting to situate the concept within a philosophical understanding of the fundamental right of individuals. The absence of a definition of privacy is a common characteristic of all of the legislation discussed in this section.

The report goes on to encourage the development of vital 'statutory protections' for the privacy of Canadians by developing the Act into a "broad-based vehicle for protecting a wide range of privacy rights", proclaiming that "(n)o longer should the Act remain solely a data protection statute" (Thacker 72). While this is short of officially recommending that privacy become a constitutional right, the Committee responsible for the report believes that the Act serves to extend rights, in this case, the right to privacy of personal information shared with the federal government (Thacker 5). Finestone's report, published 10 years later, also criticized the Privacy Act for being too narrowly focused on data protection and called strongly for the inclusion of privacy as a fundamental right in the Charter (2, 31).

The Supreme Court has recognized that the Privacy Act can be purposively interpreted as 'quasi-constitutional', and that the Act itself is a "reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society" (*Lavigne v. Canada* 789). A purposive interpretation means that the courts can consider not just the wording of the Act itself, but also the intention of the Act as documented in the secondary materials that are a result of the legislative process that created the Act (Sullivan 269). This can include documents tabled during the legislative process, reports to Standing Committees, or the transcripts of Hansard, among other resources (Sullivan 659). Quasi-consitutional Acts are those that express values that are so fundamental that they can override other inconsistent laws (*Guide to Federal Acts* 33). They are 'quasi-constitutional' because they support rights that are not included in the Charter, yet are important enough to be given special consideration by the courts (*Guide to Federal Acts* 36). What this means is that the protection of personal information shared by individuals with the federal government is less than a constitutional right but more than a legal obligation.

Ultimately, it is the Treasury Board Secretariat that manages the supervision of government-held personal information (Finestone 27). While they issue data protection guidelines to government departments based on the Act, there is no mechanism to ensure compliance (Finestone 27). In fact, according to the current Privacy Commissioner David Therrien, government departments have no obligation to report privacy breaches to the Office of the Privacy Commissioner, and there are no explicit physical, organizational or technical requirements for the safeguarding of personal information, other than the fact that it must be done ("Letter to the Standing Committee").

Therrien does consider privacy to be a right in Canada and calls for more enforcement powers ("Letter to the Standing Committee"). As he strongly states in his March 2016 letter

to the Standing Committee on Access to Information, Privacy and Ethics, "(e)very right needs a remedy in order to have meaning. This is especially so with respect to a fundamental right such as privacy". This exact statement was made by former Privacy Commissioner Jennifer Stoddart in 2008 (*Proposed Immediate Changes*).

The Privacy Act is responsible for regulating matters of privacy as they relate to personal information held by the federal government, but there are other federal statutes that regulate other aspects of privacy, such as the Criminal Code, the Telecommunications Act, and the Personal Information Protection and Electronic Documents Act.

Criminal Code

Section 162(1) in Part V of the Criminal Code protects against voyeurism by making it an offence to make a visual recording of a person in circumstances that give rise to a reasonable expectation of privacy. This applies primarily to situations involving nudity or sexual activity. There is an exemption in the case of peace officers who have obtained a warrant (s. 162(3)).

Part VI of the Canadian Criminal Code protects against the invasion of privacy involving the interception of private communications (s. 184). It is an offence, punishable by up to five years, for anyone to willfully intercept private communications through the use of a technical device (s. 184(1)) without the consent of one of the parties or a warrant (s. 184(2)(a,b)). There is no such prohibition against secretly taking photographs or video with no sound, though this is covered by s. 162(1) if the recording is voyeuristic in nature.

According to the Criminal Code, private communication means:

> any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it (s. 183).

This definition of private communication is as close to a definition of privacy as any of the Acts discussed in this section include. Both of the Criminal Code protections rely heavily on the concept of 'reasonable expectations', much like the Charter of Rights and Freedoms.

Protection of Canadians from Online Crime Act

In 2014, an amendment to the Criminal Code known as Bill C-13, or the Protection of Canadians from Online Crime Act, came into force. It expands on s. 162(1) of the Criminal Code with the addition of a clause which makes it a crime to publish, distribute, transmit, sell, make available, or advertise an intimate image of a person knowing that the person depicted in the image did not give their consent (Bill C-13, cl. 3).

The addition in the Criminal Code of s. 487.0195(1) allows for peace officers or public

officers to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing (Bill C-13, cl. 20). Furthermore, requests can not only be made by peace officers, but public officers, which includes who is anyone who is appointed or designated to administer or enforce a federal or provincial law (Bill C-13, cl. 20).

Also added, in s. 487.0195(2), is the protection from criminal or civil liability for preserving or providing data to law enforcement when that data is not prohibited by law from disclosure (Bill C-13, cl. 20).

Telecommunications Act

Section 7(i) of the Telecommunications Act states that "telecommunications performs an essential role in the maintenance of Canada's identity and sovereignty and that the Canadian telecommunications policy has as its objectives to...contribute to the protection of the privacy of persons". This Act guides the policies and regulations of the Canadian Radio-television and Telecommunications Commission (CRTC) and applies to telecommunications in Canada, which covers the emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system (s. 2(1)).

In 2006, the Cabinet issued a policy direction to the CRTC stating that the Commission should "rely on market forces to the maximum extent feasible as the means of achieving the telecommunications policy objectives" ("Direction to the CRTC", s. 1(a)(i)). This affects all of the policy objectives listed in s. 7 of the Telecommunications Act, meaning that the privacy statement in s. 7(i) is subject to economic factors.

The Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA applies to the protection of informational privacy in the private sector, and it began to come into force in stages in 2000 (s. 72, Note). The intent of PIPEDA is to "support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions". Part 1 of the Act is concerned with the protection of personal information collected by the private sector (s. 3), while Part 2 is focused on the electronic transmission of documents and electronic records (s. 32).

Part 2 of PIPEDA has almost nothing to do with privacy; its focus is on the regulation of the use of electronic alternatives over paper documents where communication with the federal government is concerned (s. 32). Despite the focus in this Part on 'electronic commerce', PIPEDA does not provide an explicit definition of the word 'electronic'. The Act defines 'electronic document' as "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device", while 'data' is defined as "representations of information or concepts, in any form" (s. 31(1)).

While PIPEDA was influenced in part by the OECD guidelines on transborder flows of data, it was also influenced by the European Union Data Protection Directive, which requires

countries in the EU to refuse the transfer of personal information to countries outside the EU without an assurance that the data will be adequately protected (Stoddart). In 2001, the European Commission decided that PIPEDA provided this protection (Stoddart).

The first version of the Act defined personal information simply as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization" (s. 2(1)). This differs from the Privacy Act slightly, as it doesn't contain the phrase 'recorded in any form', which is included in the Privacy Act definition. The aspect of 'electronic commerce' in the Act's description originates from the provision for federal trade and commerce in s. 91(2) of the Constitution Act, 1867 (McIsaac, Shields, and Klein 1.3.3). This provision allows the federal government to regulate matters that affect the country as a whole, which includes the jurisdiction to regulate matters provincially (McIsaac, Shields, and Klein 1.3.3).

In the name of consistency and federalism, PIPEDA does not apply to organizations already covered by provincial or territorial privacy legislation, as long as the legislation is 'substantially similar' to PIPEDA (McIsaac, Shields, and Klein 1.3.3; PIPEDA, s. 26(2)(b)). According to Industry Canada (which is now known as Innovation, Science and Economic Development), substantially similar means that the provincial/territorial legislation will incorporate the 10 principles in Schedule 1 of PIPEDA; "provide for an independent and effective oversight and redress mechanism with powers to investigate"; and "restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate" (Simpson 2388). Substantially similar privacy legislation exists in Alberta, British Columbia, Ontario and Quebec, while New Brunswick and Newfoundland and Labrador are substantially similar with respect to respect to personal health information custodians (McIsaac, Shields, and Klein 1.3.3). Though regardless of the existence of substantially similar legislation, PIPEDA applies in all provinces to federal works and undertakings (s. 30(1)), these include businesses like banks, airlines, railways, telecommunications companies, and any work "declared by Parliament to be for the general advantage of Canada or for the advantage of two or more provinces" (s. 2(1)).

In provinces without substantially similar privacy legislation, PIPEDA applies to the collection, use and disclosure of personal information by federal works and undertakings and by local works and undertakings (McIsaac, Shields, and Klein 1.3.3; PIPEDA, s. 2(1)). This means that the Act applies to any non-government business or organization in provinces without substantially similar privacy legislation that engage in 'commercial activities' (PIPEDA, s. 2(1)). According to the Act, commercial activities are "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists" (s. 2(1)). PIPEDA also applies to personal information in interprovincial (s. 23) and international transactions (s. 23.1).

PIPEDA does not apply to the collection of personal information for any purpose other than commercial activities. This exempts information collection for journalistic, artistic, or literary purposes (PIPEDA, s. 4(2)(c)).

Like the Privacy Act, PIPEDA regulates the collection, use, disclosure, and disposal of personal information. Part 1 of PIPEDA is influenced by the OECD guiding principles and the Canadian Standards Association Model Code for the Protection of Personal Information (McIsaac, Shields, and Klein 1.3.3). The core principles in PIPEDA are: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance (PIPEDA, Schedule 1, s. 4.1 - s. 4.10).

PIPEDA also depends heavily on the concept of 'reasonable expectations' and the 'right to privacy'. The purpose statement of the Act proclaims that "in an era in which technology increasingly facilitates the circulation and exchange of information" the Act recognizes the "right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances" (s. 3).

Despite the characterization of informational privacy as a right, PIPEDA includes several notable exemptions in the area of consent. The majority of these exemptions focus on providing information for the purposes of national security, law enforcement, or the courts (PIPEDA, s. 7(3)), but consent is also not necessary if the collection is "clearly in the interests of the individual and consent cannot be obtained in a timely way" (PIPEDA, s. 7(1)(a)).

PIPEDA is under the purview of the Privacy Commissioner (PIPEDA, s. 12.1), much like the Privacy Act. Under PIPEDA, the Privacy Commissioner can receive and investigate complaints (s. 12) and issue reports (s. 13). The Privacy Commissioner is also responsible for public education about the Act, and the promotion of policy development and compliance for organizations subject to the Act (s. 24). While the Privacy Commissioner does not have any enforcement capabilities, the Federal Court of Canada has the power to issue rulings and make orders based on the Act (s. 16).

Though the wording of the Act implies an individual's right to the privacy of their personal information as it relates to commercial activities, PIPEDA has not been recognized by the courts as having quasi-constitutional status. The Federal Court of Canada has acknowledged that PIPEDA is a "fundamental law of Canada" (*Eastmond v. CPR,* para. 100) in a ruling that has been cited with approval in several cases (*Leading by Example* 17). The reliance of PIPEDA on the concept of an individual's reasonable expectation of privacy has been disputed by the Supreme Court of Canada (*R. v. Spencer* 215). This topic will be discussed in detail in the next section.

The Digital Privacy Act

The Digital Privacy Act, or Bill S-4, is an amendment to PIPEDA that partially came into force in 2015. The key aspects of this amendment include a breach notification requirement (cl. 10.1) and a breach record keeping requirement that requires organizations to keep and maintain records on information breaches (cl. 10.3), neither of which has yet to come into force (cl. 27); it includes more consent exemptions, primarily in the area of business and employment transactions (cl. 7); and a clarification of the meaning of 'valid consent' (cl. 5).

This last point specifies that an individual's consent to the collection, use or disclosure of their personal information is valid only if "it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting" (cl. 5). This differs from the original wording in PIPEDA that required organizations to make a reasonable effort in ensuring that an individual is advised of the purposes of information collection and use; essentially this change was a shift from a subjective understanding of consent, to an objective one (Gratton).

Bill S-4 also changed the definition of personal information, which is now simply "information about an identifiable individual" (cl. 2(1)).

Returning to Finestone's metaphor from the beginning of this section, privacy legislation in Canada truly is a 'patchwork garden full of weeds' (26). The explicit protection of personal information is the overwhelming focus of every privacy regulation and law in Canada. Privacy was not included as a right in the Canadian Charter of Rights and Freedoms, and although the Privacy Act and PIPEDA have been interpreted as having a special or fundamental status in Canadian law, they both still suffer from a severe lack of enforcement capability by a Privacy Commissioner who is limited to publishing reports and recommendations.

Despite years of recommendations by MPs, lawyers, and Privacy Commissioners in support of broadening the concept of the privacy debate in Canada beyond that of data protection, none of the laws currently attempt to define privacy, even in the narrowest sense of the privacy of information.

The next section of this chapter will explore the challenge of defining privacy by examining the philosophical and legal scholarship that has informed major federal publications and legal decisions on privacy.

2.2 Definitions and Taxonomies

If the legislation concerning the privacy of Canadians does not define the word privacy, how can we understand what it means to have privacy and what is harmed when we don't have it?

The concept of privacy has been discussed and debated for centuries, creating a scholarship that is comprehensive in both depth and breadth. This section will focus on an examination of some of the historical and contemporary definitions of privacy as they relate to the Canadian government and the formation of Canadian legislation. This includes a further review of major federal publications and legal decisions on privacy, as well as an introduction to the scholarship and philosophy that informed those publications.

This section will introduce definitions of privacy gleaned from Canadian governmental publications and Supreme Court decisions, in some cases tracing those meanings back to seminal publications on the philosophy of privacy. The idea of privacy as 'the right to be left alone' will be discussed, and the concept will be clarified through the taxonomies introduced in the section. And finally, this section will end with an examination of the concept of a 'reasonable expectation of privacy' in the context of Canadian privacy law.

A Review of the Literature

The Task Force on Privacy and Computers

Perhaps the most seminal document in the landscape of privacy literature in Canada is a report written by a group colloquially known as the Task Force on Privacy and Computers. The Task Force was formed in 1970 by the Department of Communication and the Department of Justice with the intention of exploring the multi-dimensional nature of privacy in Canada. Their report, published in 1972, was a response to the growing use of computers and 'databanks' that stored personal information about Canadians (Task Force 2). They identified 10 major study areas, ranging from the information processing practices of government, public and private institutions; judicial, administrative and self-regulatory remedies; constitutional and international considerations; and a philosophical investigation into the multiple dimensions of the nature of privacy (Task Force 2). The report distinguished between two distinct notions of privacy: the first concerns what the authors consider to be the interrelated issues of accuracy, access, control of dissemination, and security, while the second includes the philosophical and ethical questions surrounding the nature of privacy itself (Task Force 3).

The willingness of the Task Force to consider the "more general and less tangible" aspects of privacy (3) comprises exactly the kind of discourse that Thacker and Finestone advocated for in their respective reports, published decades after the report on *Privacy and Computers* was released. The Task Force did not consider the specific concerns relating to accuracy, access, control, and security to be worthy of a fundamental conceptual analysis (3), though these issues tend to dominate the modern legislative debates surrounding privacy.

An Introductory Taxonomy

A recurring theme in the scholarship of privacy are taxonomies. Taxonomies are helpful,

as they serve to divide big concepts into smaller and more manageable parts. The Task Force on Privacy and Computers developed one such taxonomy, splitting the concept of privacy into three major categories: territorial, personal, and informational (13).

Territorial privacy relates to physical property and space. This is the idea that what happens behind walls or closed doors is one's own business, and furthermore, that no one may enter that private domain without permission, or without a lawful warrant for access (Task Force 13). Territorial privacy is perhaps the most foundational or traditional concept of privacy (Warren and Brandeis 193), and breaches of this type of privacy are some of the most easily identified: such as an intruder in or around one's home, or the presence of recording devices. The invasion of territorial privacy may even extend to noxious odors or loud noises that interrupt the solitude of tranquility of one's own space (Task Force 13; Warren and Brandeis 193). Alan Westin, a well-known privacy theorist, argues that the function of territorial privacy serves to protect individual well-being and small group intimacy, something that is found not only in humans, but in other non-human animals (9).

Personal privacy is also a spatial or territorial concept, but one that is less defined by walls or physical barriers, and more by legal norms and social values (Task Force 13). While personal privacy involves freedom of movement and the prohibition of physical assault or warrantless search and seizure (Task Force 13), it also includes the more abstract notions of personal dignity and reputation (Warren and Brandeis 194). This has been characterized as an issue of personal autonomy, or the 'right to be left alone' (Stefanick 6). While being 'left alone' is itself open to interpretation, this idea generally refers to the moral rights one has over one's own body, in terms of freedom of expression and freedom from intrusions that blur the boundaries between one's personal and social life (Richardson 30; Stefanick 6; Warren and Brandeis 194).

Informational privacy is the most abstract of these three distinctions, and in some ways it encompasses the previous the concepts of territorial and personal privacy, especially in terms of modern technology. For example, the digital addresses associated with networked devices can provide information about an individual's physical location, and social media has the ability to affect the reputation of an individual if others post information that cannot be removed or altered. As evinced by the previous section, informational privacy is also the primary type of privacy protected by most of Canada's privacy legislation.

Informational privacy refers to the ability for an individual to have control over the ways in which information about the self is disclosed. This is based on an assumption of ownership, meaning that information about a person belongs to that person, and can be used in whatever way that person sees fit (Task Force 13). But much like privacy, the concept of information is in itself difficult to define. Before undertaking an examination of informational privacy, we must first understand what is meant by the word 'information'.

What is Information?

Claude Shannon, known as the 'father of information theory' (Floridi, *Information* 1) puts forth a broad definition. He defines information as:

> the messages occurring in any of the standard communication mediums such as telegraphy, radio or television, the signals involved in electronic computing machines, servomechanisms systems and other dataprocessing devices, *and even the signals appearing in the nerve networks of animals and man*. (emphasis added, Shannon 212)

Luciano Floridi builds on Shannon's definition with his own philosophy of information, describing the current state of information in society as the 'infosphere'. The infosphere is "the whole system of services and documents, encoded in any semiotic and physical media, whose contents include any sort of data, information, and knowledge" ("The Digital Revolution" 8). It is the whole informational environment and all of its constituent entities including "their properties, interactions, processes, and mutual relations" ("Foundations of Information Ethics" 3).

Floridi has a useful analogy to describe this concept of the 'infosphere'. He asks us to imagine the universe from a chemical perspective; everything within it has a chemical composition such as humans are 60% water, or the air is made up of mostly nitrogen and oxygen. In this way, the world can also be imagined from an informational perspective. The same entities described by their chemical composition can be described by their informational composition. Therefore, every 'thing' is information, and "to be is to be information" (Floridi, "A Defence of Informational Structural Realism" 241).

Combining Floridi's concept of the infosphere with Shannon's definition of information, we can conclude that if every 'thing' is information, then everything about a person, from the physical to the abstract, is personal information.

This comprehensive view of personal information is less robust than the definitions provided by federal privacy legislation, namely that personal information consists of "information about an identifiable individual" (PIPEDA, s. 2(1); Privacy Act, s. 3). The Office of the Privacy Commissioner of Canada considers personal information to include things like SIN numbers and other numbers associated with identification, birth dates, addresses, names, banking information, fingerprints and even IP addresses ("Your Guide to PIPEDA"). Each of these items, even something as abstract as a SIN number, is a surrogate for something physical that exists in the real world. A SIN number represents one's uniquely physical identity with the Canadian government, an IP address refers to an actual, physical networked device like a computer or a smartphone. These examples show how easy it is to make connections between specific pieces of information and an individual in the tangible, physical world.

We are increasingly beginning to amass a considerable amount of personal data that does not have a real-world manifestation. This can include data like web browsing histories, health tracking information collected by wearable fitness devices, credit reports, academic applications and transcripts, and 'profiles' generated by data aggregation algorithms owned by Google or Facebook. This information is more connected to the personal behaviours of individuals, rather than the physicality of the individual themselves. The data often includes a web of other connected and related data, even temporal and spatial information like timestamps or GPS coordinates. Some of this data is collected remotely and outside of Canada, recorded on a

variety of different mediums and in different formats, and in some cases, protected by Terms of Use agreements that render identification and ownership unclear.

While information that is considered 'personal' by the Canadian privacy legislation is protected when collected for the purposes of government or commercial use, there are many other types of secondary and less tangible personal information that has no such explicit protection.

Our first taxonomy has established that privacy applies to three domains: the territorial, the personal, and the informational. Using this taxonomy, I have suggested that territorial and personal privacy are really just types of informational privacy, because information about a physical location, and information about an individual are both just different types of information. Furthermore, we have the argument from the Task Force that informational privacy means that information about a person belongs to that person, and its transmission or communication should not only be protected, but controlled by the individual themselves (13). Finally, the definitions of information put forth by Shannon and Floridi have established that everything about an individual is comprised of information, down to the smallest details of internal biology, such as the electrical messages transmitted by the nervous system (Shannon 212).

A Second Taxonomy

Where the first taxonomy recognized three different theoretical 'spaces' of privacy, Westin has developed a taxonomy that differentiates between individual 'states' of privacy. The difference here is subtle. Westin is not focused on the spaces where privacy is said to exist, but rather the basic functions that privacy serves for individuals and groups in society (31). These states of privacy are solitude, intimacy, anonymity, and reserve (Westin 31).

Solitude simply means separation, where an individual is separated from the group and from the observation of others (Westin 31). This state, according to Westin, is the most complete state of privacy that can be achieved (31).

Intimacy, the second stage of the taxonomy, is less private than solitude, and occurs when an individual is a part of a small unit that enjoys seclusion within a close and relaxed relationship (Westin 31). This includes marriages or partnerships between people, families, circles of friends, or even work cliques (Westin 31).

Privacy as anonymity is freedom from identification and surveillance, even in public spaces (Westin 31). Even if the individual is aware of being observed, anonymity means that the observation occurs without recognition or identification, letting the individual have the ability to "merge into the situational landscape" (Westin 31). Also included in the state of anonymity is the freedom to publish ideas without identification (Westin 32). Anonymity can be understood as a form of 'public privacy', where an individual is free to negotiate societal expectations while remaining free from recognition or identification. A further discussion of anonymity will follow later in this section.

The last state of privacy is reserve, which Westin considers to be the most subtle of

the four states (32). Reserve protects against unwanted intrusions with the creation of a 'psychological barrier' in the mind of an individual, serving the purpose of protecting certain aspects of the self from others (Westin 32). This type of privacy allows a person to cultivate a 'mental distance' within intimate relationships and public life. To Westin, reserve is essential to an individual's sense of meaningful privacy, especially in an urban, industrialized society (32).

Westin's taxonomy of the states of privacy informs a further taxonomy regarding the functions of privacy for an individual in society. The relationship between privacy of the individual and society, as well as Westin's functional taxonomy, will be discussed in the next section of this chapter.

A Third Taxonomy

In a decision known as *R. v. Spencer*, s. 8 of the Canadian Charter of Rights and Freedoms was used by the Supreme Court in a ruling involving informational privacy.

While *R. v. Spencer* was heavily influenced both by Westin and by the Task Force on Privacy and Computers, the ruling also introduced its own taxonomy of privacy. The judgment stated that in order to understand informational privacy, the nature of privacy itself must itself be understood in three contexts: privacy as secrecy, privacy as control, and privacy as anonymity (*R. v. Spencer*, para. 38).

Privacy and secrecy are aspects of confidentiality. A straightforward example of this concept relates to medical records. While people may share private information to receive medical care, they retain an interest in the protection and confidentiality of that information (Task Force 14). The relationship between the information-giver and the information-receiver, such as the one between a patient and doctor, depends on the information-giver having a reasonable expectation that the information-receiver will hold the information in confidence (*R. v. Spencer*, para. 39). The information exchange depends completely on trust; trust that the information will be kept completely secret from those outside the relationship. Another Supreme Court ruling, *McInerney v. MacDonald*, describes the patient-doctor relationship as fiduciary, meaning that a doctor has a duty to hold information received from a patient in confidence, and a patient has the right to expect that the duty of the doctor will be fulfilled (149, para. i).

Privacy as secrecy is primarily covered by the collection, purpose, and use provisions in Canadian privacy legislation. In other words, personal information is collected and used for a specific purpose with the express consent of the individual, and disclosure to others does not occur except with consent or lawful authority.

Privacy as control refers to the ability for an individual to determine how their personal information is used, if at all (Stefanick 29; Westin, *Privacy and Freedom* 7). This differs from the idea of privacy as secrecy, because the communication of certain types of personal information is often necessary beyond the intimacy of relationships such as the ones between a doctor and patient, or a lawyer and client. Privacy as control is related to an individual's reasonable expectation of the privacy of their personal information, and their ability to determine and

restrict its disclosure (*R. v. Dyment* 429, para. i).

Privacy as control is covered by the consent, disclosure, and safeguards provisions in Canadian privacy legislation, along with the collection, purpose, and use provisions discussed above.

Privacy as anonymity, in the context of *R. v. Spencer*, borrows strongly from Westin's idea that individuals should be free from recognition or identification in public places, as well as freedom to publish ideas without identification (*R. v. Spencer*, para. 43, para. 45; Westin, *Privacy and Freedom* 31). Even though *Privacy and Freedom* was published in 1970, Justice Cromwell argues that Westin's idea of anonymous publishing perfectly defines many contemporary characteristics of internet communication and use (*R. v. Spencer,* para. 45). The internet is a functional extension of the concept of 'public space' in society, and while an internet user may not necessarily be able to control the monitoring or observation of their online activities by outside actors, they should have the ability to remain anonymous in that space, without having their personal information disclosed and linked to their online activities (*R. v. Spencer*, para. 47).

Justice Cromwell argues that it is crucial that the link between personal information about an individual and the behaviours or activities in which the individual participates should be protected by a degree of anonymity (*R. v. Spencer*, para. 50). The reasoning behind this is articulated by Slane and Austin, who describe the difference between personal information about identity (such as a name or a phone number) and personal information that serves the purpose of identification (500). Information like names and addresses are rarely completely private, a phone book is a good example of this, but information used for identification, such as a SIN, has the ability to link an individual to many other types of information, like financial and tax history (Slane and Austin 501). Anonymity is not the freedom to keep every single piece of information about the self private, but the freedom from having that personal information lead to identification, which can then lead to the disclosure of information of a more intimate and personal nature.

What this amounts to, a broad sense, is that privacy can be conceptualized as the right to choose anonymity, or perhaps as the right to be left alone.

The Right to be Left Alone

It may be that the first 'modern' taxonomy of privacy was developed in 1890 by American legal scholars Samuel Warren and Louis Brandeis. While it was understood at the time that privacy was a territorial and personal concept, they argued that if the law could protect the rights of property and corporeality, it could also protect the "intangible products and processes of the mind" (194). They believed that the protection and security of the individual amounted to the right to be left alone (194).

Frustrated over the ability of the news media to obtain and disseminate photographs of his daughter's wedding, Brandeis later wrote in a 1928 US Supreme Court ruling, *Olmstead v. United States*, that the "greatest dangers to liberty lurk in insidious encroachment by men

of zeal, well-meaning but without understanding" (479). This statement is an extension of his earlier work with Brandeis, which argued that an "absence of malice" is no excuse for violating the privacy of others, forwarding the idea that a violation of informational privacy may result in the harm of one's dignity, despite the intentions of those seeking the information (Warren and Brandeis 218).

While it is relatively easy to determine whether a territorial or personal violation has occurred (e.g., someone digs through your trash on your property, finding a personal letter or photo and publishes it), it is less obvious when informational privacy has been compromised, unless something like identity theft or hacking occurs. This raises the question from the beginning of this section: what harm is there in the sharing of information, especially if the person whose information was shared never finds out?

If breaches of informational privacy weren't harmful in some way, there would be no reason for the Canadian justice system to rule on cases involving the disclosure of personal information. Yet even though privacy is narrowly recognized in Canadian law as the quasi-judicial or fundamental protection of personal information held by government and business, there is no shortage of examples from case law recognizing the harm of the unnecessary invasion of personal privacy.

Often these cases hinge on whether or not the claimant had a reasonable expectation to the privacy of their personal information. As discussed in the previous section, reasonable expectations form the basis of much of the privacy legislation, from PIPEDA to the Criminal Code.

What is a Reasonable Expectation of Privacy?

R. v. Spencer

As mentioned above, *R. v. Spencer* used s. 8 of the Canadian Charter of Rights and Freedoms in a ruling involving informational privacy. Section 8 of the Charter is one short sentence, stating that "(e)veryone has the right to be secure against unreasonable search or seizure". The court case was about the justification for warrantless access to personal information; specifically whether the police were justified, under PIPEDA, in requesting from an internet service provider (ISP) information about a subscriber associated with an IP address, without first obtaining a warrant from the appropriate judicial authority. The Supreme Court unanimously agreed that the request by the police for this information without a warrant was unconstitutional (*R. v. Spencer* 215). They ruled that internet subscribers have the right to a reasonable expectation of privacy concerning their personal information (para. 66), because the activities that individuals engage in online carry with them an expectation of anonymity (para. 44).

In the case, the internet user was accessing and downloading child pornography on a computer belonging to a family member (*R. v. Spencer*, para. 7). The police became aware of the activity because of the individual's use of file-sharing software, and they subsequently requested subscriber information including the name, address, and telephone number from the ISP, in this case Shaw Communications Inc. (*R. v. Spencer*, para. 8). Section 7(3)(c.1)

(ii) of PIPEDA states that "an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is requested for the purpose of enforcing any law of Canada", while s. 5(3), states that "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances".

There is a circularity here between these two sections, where s. 7(3)(c.1)(ii) depends on s. 5(3) in terms of an understanding of the concept of 'reasonable'. Ultimately, the issue was not whether or not a crime was committed, but rather if the police were justified in accessing personal information without either the consent of the individual, or a warrant. As s. 8 of the Charter ensures the right to be secure from unreasonable search or seizure, the constitutional foundation of this case asks if the police request for personal information was an unreasonable search. According to Justice Cromwell, writing for the Court in *R. v. Spencer*, "the answer to this question turns on whether, in the totality of the circumstances, Mr. Spencer had a reasonable expectation of privacy in the information provided to the police by Shaw. If he did, then obtaining that information was a search" (*R. v. Spencer*, para. 16).

Determining whether there is a reasonable expectation of privacy is the key to the use of s. 8 in a constitutional claim for the right to privacy (McIsaac, Shields, and Klein 2.3). When there is no reasonable expectation of privacy, there is no constitutional right to be secure from an unnecessary search. In the case of *R. v. Spencer*, the Supreme Court ruled that a degree of anonymity is foundational to the understanding of privacy, and that a person can reasonably expect privacy when using the internet, despite what that use may entail.

In other words, a reasonable expectation of privacy amounts to a reasonable expectation of anonymity.

A narrow view of this interpretation of privacy as anonymity comes from a speech made by Justice Sopinka of the Supreme Court, discussing his views on the another similar case, *R. v. Plant*. He states that "(t)he more accessible the information about an individual, the less is his or her expectation of privacy" ("Freedom of Speech and Privacy"). Justice McLachlin, who dissented the ruling, stated in the judgment that information should only be used explicitly for the purpose in which it was collected, and that disclosure beyond the bounds of that purpose should only be undertaken with proper legal authorization (*R. v. Plant* 283, para. h).

These opposing views highlight the contradiction between the right in s. 8 of the Charter to be free from unreasonable search and seizure, and the consent and disclosure exemptions in federal privacy legislation that arguably allow for warrantless access to personal information. This contradiction is what makes the case of *R. v. Spencer* so compelling.

Justice Cromwell alludes to this contradiction in the ruling, stating that "Section 7(3)(c.1)(ii) of PIPEDA cannot be used as a factor to weigh against the existence of a reasonable expectation of privacy since the proper interpretation of the relevant provision itself depends on whether such a reasonable expectation of privacy exists" (214-215). Cromwell characterizes PIPEDA as a piece of legislation that is meant to protect the personal information of individuals

by restricting non-consensual disclosure, and not as a legal tool for the warrantless access of information by law enforcement (215).

Yet, *R v. Spencer* is only one Supreme Court decision out of many. An understanding of what a 'reasonable expectation of privacy' actually is continues to be decided, literally, on a case by case basis.

While an understanding of the meaning of privacy is important to the interpretation of privacy legislation, it is also just as essential to understand the function that privacy serves to individuals and to society. The next section will investigate this topic by examining another of Westin's taxonomies, along with a discussion of the kinds of harms that can be sustained from privacy violations, and the lasting impacts of the erosion of privacy on society.

2.3 The Function of Privacy

If privacy served no function in society, there would be no need to create legislation to mandate its protection. In the words of the Task Force, "(i)n a world of total social cohesion and mutual trust, privacy might be unnecessary" (18). And even though Westin argues that privacy is a fundamental need, found both in humans and animals (9), this perception of privacy relies heavily on the spatial and personal concept of privacy, rather than the informational.

But as evinced by earlier sections of this chapter, informational privacy is the primary type of privacy protected by Canadian law. The law ensures that individuals have a claim to a reasonable expectation of the privacy of their personal information when it is obtained for government or commercial activities. Based on the examination of the phrase 'reasonable expectation of privacy' in the last section, an expectation of privacy is really an expectation of anonymity. This means that an individual may expect to be identified, but not identifiable by their personal information. The nuance between these terms, according to Slane and Austin, is in the understanding that there is a difference "between information that discloses substantive details about an individual's identity and information that is used as an 'identifier'" (500).

While a name, phone number, or address may be easily obtained by searching a phone book, other types of personal information are more related to a person's 'biographical core'. This type of information, according to Justice Sopinka in the ruling of *R. v. Plant*, can reveal "intimate details of the lifestyle and personal choices of the individual" (293, para. h). It is precisely to what extent this type of personal information needs protecting that the case of *R. v. Spencer* and others sought to determine.

The purpose of this section is to examine the function of informational privacy by revisiting two of Westin's 'states of privacy', as well as his taxonomy of the function of privacy in society. This will be integrated with the taxonomy presented in the last section by *R. v. Spencer*. These interrelated concepts of privacy will be used to counter the 'nothing to hide' argument, which claims that privacy is unnecessary if one has nothing to hide. This section will end by returning to the philosophical questions posed by the Task Force concerning informational privacy and power.

Two of Westin's four states of privacy--anonymity and reserve (31)--relate closely to another of his taxonomies examining the function of privacy for individuals in society. These functions are: personal autonomy; emotional release; self-evaluation; and limited and protected communication (Westin 32). As a review from the last section, the taxonomy of privacy presented in *R. v. Spencer* consists of privacy as secrecy, control, and anonymity (para. 38).

Personal autonomy, according to Westin, is "the desire to avoid being manipulated or dominated wholly by others" (33). This is achieved by keeping one's "core self" private by sheltering the "ultimate secrets" of one's hopes and fears from the view of even the most intimate companions (Westin 33). This is closely related to the state of reserve, or the psychological barrier in the mind of an individual that protects certain aspects of the self from

others (Task Force 17; Westin, *Privacy and Freedom* 32).

Personal autonomy is also vital to the maintenance and development of one's personal identity and sense of individuality (Westin 34). In this way, personal autonomy is closely aligned with privacy as anonymity and control. Without the freedom to experiment with thoughts and opinions anonymously, one may be subject to ridicule and shame by others, or worse, be subject to the control of those who know one's secrets (Westin 33-34).

This argument for the necessity of privacy for the development of the self is not unique to Westin. In the 1800's, John Stuart Mill argued in *On Liberty* that even in a perfectly representative democracy, individuals still need a space where they are free from the intrusion and will of the government and society (9). He introduced the idea of the 'tyranny of the majority' (Mill 10). The majority, or society itself, mustn't have the power to impose "its own ideas and practices as rules of conduct on those who dissent from them" (Mill 10). What Mill is saying is that in a society where the majority has the power to elect the government, there also exists the power to influence other domains through custom and tradition. Individuals should be able to participate in society, while also having the right to retreat to a realm free from the influence of others.

Personal autonomy is threatened when others gain access to this core self, either purposefully or by accident. The dangers of accidental breaches of privacy are perhaps most famously articulated by Brandeis, writing that the well-meaning collection of information by the government is the most dangerous when conducted by those with excitement and good intentions, but a lack of understanding (*Olmstead v. United States* 479).

Emotional release refers to the ability for an individual to have moments "off stage" as a relief from the variety of roles that life demands (Westin 35). This relief can manifest in several different ways: as the freedom to 'turn off' after work or social obligations; as the ability to take a break from social or institutional norms of behaviour; as the opportunity to vent anger or frustration at 'the system; or as the ability to manage bodily and sexual functions (Westin 35-36). If all of a person's private transgressions were known, whether they are thoughts or behaviours, most people would be constantly facing the threat of punishment or scorn (Westin 35). The anonymity of emotional release allows people to function in society without fear of criticism or interference by others. This can also be viewed as the link between privacy and secrecy, where one may choose not to share personal information with anyone, even intimately.

Self-evaluation, Westin's third function of privacy, allows individuals to take stock of their feelings, needs, and experiences in order to evaluate and then assert their independence (Westin 36-37). This function is closely related to reserve, in that privacy allows an individual to consider the alternatives and possible consequences of their actions before deciding how much of themselves to share with the world (Westin 36-37). This function of privacy relates to both the concepts of secrecy and control. One may spend time evaluating the self in secret, only to carefully control the aspects they wish to reveal after periods of reflection and deliberation.

And finally, the function of limited and protected communication concerns both anonymity and reserve, in that it provides an individual with the ability to share confidences with intimate companions, or with no one at all (Westin 38). This applies to the concept of privacy as secrecy, control and anonymity, where the disclosure of personal information requires a substantial degree of trust, such as in relationships like those between doctors and patients, or lawyers and clients.

What these functions of privacy add up to is the argument that privacy is essential to the development of a person's complete and unique sense of self; as an individual, as a participant in intimate relationships; and in relation to society as a whole. Privacy allows individuals to 'test out' feelings, thoughts, and points of view without the fear of scorn, shame, or judgment, from the government or from the public.

Personal autonomy, emotional release, self-evaluation and the limiting or protecting of communication no longer occur only behind the physicality of closed doors. Almost every activity in daily life can now be recorded and stored as data in some way. A non-exhaustive list includes public and private surveillance cameras; textual communication like email, chat, or text messaging; web browsing histories and bookmarks; personal devices that track location, speed, sleep, and heart rate; automated payroll and tax filing services; online banking; and numerous other activities essential and unavoidable in daily life. This is all personal information, and taken as a whole, it can lead to a very complete and identifying picture of an individual's biographical core.

At the individual level, widespread surveillance can result in what the Task Force describes as conformist behaviour, which is "induced by the certainty that one's file exists and grows, coupled with the uncertainty as to what it contains and the uses to which it will be put" (18). When an person is aware that they are being observed, or even that there is a chance they are being observed, they may decide to change their behaviour or refrain from certain types of activities entirely (Westin 58). This is referred to as the 'chilling effect of surveillance', and it is harmful not just to individuals, but to society as a whole (Solove 765). The societal harm is in the narrowing of the expression of a range of viewpoints, thoughts, and opinions, and the decreasing freedom to participate in political activities (Solove 765).

Another potential harm from the collection and processing of large quantities of personal information are the effects of data mining. Data mining, or 'knowledge discovery in databases' (KDD), is the "non-trivial extraction of implicit, previously unknown, and potentially useful information of data" (Frawley, Piatetsky-Shapiro, and Matheus 58). Data mining allows for the description and potential prediction of behaviour of individuals and groups through the discovery of understandable information patterns in large databases. This activity may lead to a range of potential consequences for individuals, from the classification of people into larger groups based on an indistinguishable set of characteristics, to the denial of service or penalties for certain types of personal behaviours (Vedder 276). One potential application of data mining concerns the cost of insurance; people who wear a fitness tracking device, or consent to the monitoring of their unique driving habits may qualify for less expensive policies. But the collection of this data may lead to the discovery of other personal information, like an

abnormal heart rate in the case of a fitness tracker, or the discovery that a driver may not be where they claim to be, based on the GPS logs from their vehicle. Or, as suggested by the Task Force, Westin, and Solove, the knowledge of the surveillance will simply lead people towards conformity by refraining from certain activities altogether, despite what they may desire or need.

The idea that privacy can promote the development of a person's unique sense of individuality, which in turn can lead to the flourishing of a diverse and free society, stands in clear opposition to a privacy concept known as the 'nothing to hide' argument.

"I've Got Nothing to Hide"

The 'nothing to hide' argument centres precisely on the surveillance and collection of the types of information described above. The argument, as described by Solove, is that there exists no threat to privacy as long as individuals are engaging in lawful activities (746). If surveillance uncovers illegal activity, then a person has no legitimate claim to privacy because what they are doing is wrong (Solove 747). Support for this argument rests on the logic that surveillance or data mining collects only particular types of information that will only be disclosed to a small group of people in business or government, and that the security interest in the collection of this information is higher than the embarrassment that one may feel if their privacy is breached (Solove 753).

The problem with this argument, according to Solove, is that it reduces privacy to the singular purpose of concealment or secrecy (Solove 764). While secrecy is one element of privacy, it is far from its only function. Each of Westin's four functions of privacy stands in direct opposition to the 'nothing to hide' argument. Even the act of keeping secrets does not automatically imply illegal or immoral behaviour.

This sentiment is echoed in *R. v. Spencer*. Justice Cromwell, writing for the court in a case that involved the privacy interest of a defendant accused of accessing child pornography, an undeniably immoral offence. He states that the "nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought" (*R. v. Spencer,* para. 36).

So while the 'nothing to hide' argument focuses on privacy solely as a form of secrecy, it fails to acknowledge the other types of harm that can result from the erosion or lack of privacy (Solove 767), while disregarding the important and multiple functions privacy serves for the development of individuals, and society.

Edward Snowden summarizes this debate succinctly with the following statement from an Ask Me Anything discussion on Reddit. He says that "(a)rguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Privacy and Power

The Task Force on Privacy and Computers, in their investigation of the"more general and less tangible" aspects of privacy, posed the following questions

> What is the relationship between privacy and political power? Will current and projected uses of the computer lead to loss of individuality or to enforced conformity? Is the desire for informational privacy fundamentally social or anti-social? How can a balance be achieved between claims to personal privacy and claims, as legitimate but sometimes conflicting, for unimpeded access to information? (3)

What they saw as the common thread among these questions was the ability of computing to concentrate, disseminate, and redistribute personal information among organizations and government (Task Force 19). The transfer of personal information from one place to another, to them, was a fundamental redistribution of power; a power that could be used for good or for evil (Task Force 19-20). It is incredible that while this report was written in 1972, it describes so clearly the philosophical issues underlying the modern privacy debate.

Privacy 'rights' in Canada consist of the quasi-constitutional right to the protection of personal information held for government or commercial purposes, where a reasonable expectation of privacy exists. This does not constitute an explicit right to privacy. While the courts continue to interpret Canada's existing privacy legislation in an attempt to clarify the meaning of privacy, none of the legislation provides a definition or an explanation of what privacy actually means, though meaning can be determined through the examination of Standing Committee Reports, and Supreme and lower court rulings, as the research in this section shows.

Another type of clarification can come from the description and debate provided by the authors of the legislation, the elected Members of Parliament. Sullivan states that "(w)hen the purpose of a provision is discussed or its meaning explained during the enactment process, and the legislation is then passed on that understanding, the explanation or discussion offers persuasive (if not conclusive) evidence of the legislature's intent" (659).

The next chapter will conduct a text analysis on the transcripts of Hansard, the parliamentary debates in the House of Commons, in an attempt to uncover the meaning of privacy as it is understood by the those who have the responsibility for the creation and enactment of the legislation itself, Canada's Members of Parliament.

3 Text Analysis

Text analysis, according to linguist Svenja Adolphs, offers "a way into the data that is informed by the data itself" (19). The purpose of the text analysis in this chapter is to discover trends from Hansard that would be difficult to determine from reading alone. The selection of Hansard chosen for this research contains almost 69 million words spanning ten years of governance in the House of Commons.

Text analysis is a type of research methodology that involves the study of language in texts beyond the unit of the word, clause, or sentence (McKee 1; Stubbs, *Words and Phrases* 5). Stubbs situates this definition within his assertion that our understanding of language is more than knowledge about individual words, but of the ways in which they can be combined, and the cultural knowledge that surrounds those unique combinations (*Words and Phrases* 3). For the purposes of this chapter, a text consists of spoken or written language that is naturally occurring within a real context (*Words and Phrases* 5).

Text analysis, as a methodology, can be used to determine the meaning of a word by studying the words that surround it, within the context of its use. The context of the text under analysis in this research is political discourse, specifically the language used in the House of Commons. Parliaments are institutions which have predictable patterns of spoken discourse; MPs debate, question, explain and justify in an environment of legislation and policy (Bayley 1). It is a purely linguistic activity where the result of the discourse establishes what may or may not be done in a given society (Bayley 12). Parliamentary discourse is, as Bayley describes, "a struggle over meanings" (12).

The ways in which words are used can reveal their meaning, when they are examined within the context of their use. Sinclair refers to this as the 'state of the discourse' (*Trust the Text* 14). The state of parliamentary discourse is deeply reflective of the culture of the MPs. The language reveals the relationship between the speakers and their own beliefs, expectations and evaluations of the world around them (Stubbs, *Words and Phrases* 6). In order to understand language, the speakers and the hearers must have something in common. According to Stubbs, speakers and hearers of language must share knowledge and assumptions about the world, linking their communicative competence with their cultural competence (*Words and Phrases* 6). This means that contextual knowledge about the world helps people to infer meanings from language, meanings that often transcend the dictionary definition of individual words. The methodology of text analysis can be used to define a word in the context of its use, both linguistically and culturally, determining its meaning as a joint construction of the shared knowledge between the speaker and the hearer.

Purpose of this Chapter

The purpose of this chapter is to gather information about the use of the word 'privacy' in the House of Commons in order to pinpoint areas of interest for a further critical analysis of the discourse.

Using the transcripts of Hansard, spanning the period of the 39th to the 41st Parliaments

(which cover the years 2006 to 2014), this chapter will investigate the following questions:

Word Frequencies

- What is the frequency of the use of the word 'privacy'?
- Has there been an observable change in the frequency over time?

Concordances

- What patterns of language use are visible in the output of concordances?

Overview of this Chapter

If text analysis is a research methodology that involves the gathering of data about 'texts', then electronic text analysis involves the gathering of data about electronic texts. Adolphs extends this definition to encompass not only texts, but entire collections of texts (3). While collections of text can appear in many contexts (i.e. libraries, the Internet, newspaper archives), when that collection has been assembled with the intention of linguistic analysis, it is known as a corpus (Tognini-Bonelli 2; Hunston, *Corpora in Applied Linguistics* 32). The first section of this chapter will explain what a corpus is and how it can be used for text analysis. This will be followed by a description of the Hansard corpus and the justification for its use in this research.

Section 3.2 will examine how the frequency of words in a corpus is calculated, discussing the common terms, statistical methods, and limitations of this type of research. The results of the word frequency analysis on the Hansard corpus will be revealed.

Section 3.3 will focus on the history and method of producing concordances for text analysis research. The Hansard concordances will be analyzed.

Section 3.4 will discuss the results of this chapter, and how the results will be used to inform and direct Chapter 4, which will be a Critical Discourse Analysis that focuses on one of the most compelling trends discovered as a result of this text analysis.

3.1 Corpora

The use of a corpus (or the plural corpora) for the investigation of language existed before the advent of computerized analysis, although, as we will briefly explore here, the computer had a profound effect on expanding the range of methodologies and theories involved in the practice of text analysis. But first, it is important to operationalize the term 'corpus' so that it can be better understood in the context of electronic text analysis.

Characteristics

Put simply, a corpus is a collection of texts with intention. There is a general consensus that the texts should be an authentic and balanced representation of a language within the context of its use (Adolphs 2; Baker 2; McEnery, Xiao, and Tono 21; Sinclair, *Trust the Text* 13; Tognini-Bonelli 57). Corpora may consist of spoken or written language and thus are a sample of human behaviour, but it's important to note that a sample of behaviour does not constitute the behaviour itself (Stubbs, *Text and Corpus Analysis* 233). The corpus is, according to Hunston, "neither good or bad in itself" (26), it is merely a constructed record arranged for a purpose (Hunston, *Corpora in Applied Linguistics* 26; Stubbs, *Text and Corpus Analysis* 233).

A corpus is authentic if it consists of material, as Tognini-Bonelli describes, that has been "taken from genuine communications of people going about their normal business" (55). It must be noted that it is an oversimplification to assume that every single word, phrase or sentence that occurs in the corpus is completely indicative of the language under study, because it is difficult to fully articulate what should count as 'language use' (Tognini-Bonelli 55). For this reason, the authenticity of a corpus is closely related to its representativeness. A balance exists if the language use in the corpus is generalizable to the variety of language it is meant to represent within its greater context (Baker 26; McEnery, Xiao, and Tono 21; Tognini-Bonelli 57; Yates 103).

Corpora can come in many shapes and sizes and can include whole texts or samples of texts (Baker 30; Hunston, *Corpora in Applied Linguistics* 32; Sinclair, *Corpus, Concordance, Collocation* 24). Monitor corpora grow continually, with new texts being added that are representative of the language-in-use, like newspaper archives (Baker 30; McEnery and Hardie 246; Sinclair, *Corpus, Concordance, Collocation* 26). Static or reference corpora are more generalized and discontinuous (Sinclair, *Corpus, Concordance, Collocation* 24) and they try to represent a particular type of language over a specific period of time (McEnery and Hardie 8). An example of a static corpus is the Lancaster-Oslo/Bergen (LOB) corpus, which represents a 'snapshot' of modern British English in the 1960's (McEnery and Hardie 9). Other categories of copora include: comparable corpora, which enable researchers to compare the similar content in different languages; parallel corpora, which involves translated text, the Canadian Hansard published in both English and French is a good example; learner corpora, which focus on texts produced by learners of a different language; and historical or diachronic corpora, containing texts from different periods of time that help trace the development of language or language use (Hunston, *Corpora in Applied Linguistics* 15-16).

Advances in computer processing technology have made it increasingly possible to work with larger and larger corpora, and in the words of Sinclair, this access allows for a "quality of evidence that has not been available before" (*Corpus, Concordance, Collocation* 4). But the purpose of a corpus as a research tool must always be clearly articulated. There is a distinction between what is known as 'corpus-based' research and 'corpus-driven' research. The former is concerned with deductive research, where theories about language and language use are tested and confirmed based on corpus data (Tognini-Bonelli 65). The latter has a focus on inductive research, where a hypothesis is formed based on observations made about the corpus data, and the subsequent generalizations and theories must be "fully consistent with, and reflect directly, the evidence provided by the corpus" (Tognini-Bonelli 85). The difference, in essence, is temporal. In corpus-based research, the theories come before the corpus, and in corpus-driven research the theories come after the corpus.

History

While corpus-driven research is essentially a product of the increasing availability of computer-assisted text processing, methods of text analysis pre-date the computer. The manual analysis of corpora has its origins in the 12th and 13th centuries (Adolphs 5). The earliest texts were primarily religious manuscripts, and corpus research was concerned with the production of concordances, a text analysis method that organizes the data so that a particular key word or phrase appears with a sample of its accompanying text to provide context (Adolphs 5). In the 1950's, an Italian Jesuit priest named Father Roberto Busa began a project that would ultimately give birth to the field of Humanities Computing by producing the very first computerized concordance, placing the works of St. Thomas Aquinas and others on punch cards to undergo mechanical processing (Hockey). By the 1960's, other scholars were beginning to see the potential for computer-assisted text processing for tasks such as authorship determination and ancient language research (Hockey).

Theory

Technological advances in machine readable corpora have increased the interest in the study of language and corpus-driven studies, highlighting the distinction between the empiricist and rationalist approaches to research. Empirical methods of electronic text analysis allows for the observation of trends and the creation of statistics based on naturally occurring language. The frequency of words can be counted, and concordance lists can be created and analyzed. Texts can undergo quantitative analyses that can be reproduced by other researchers. This is in contrast to the rationalist tradition of linguistics, popularized by scholars like Noam Chomsky. He argued that the focus of language study should be on 'competence' (the internalized knowledge of a language) rather than its external use, known as its 'performance' (Adolphs 6). His argument was that performance data does little to inform or reveal knowledge about competence (Adolphs 6). He also argued that there could never be a sample of naturally occurring language large enough to be a true representation of language use (Adolphs 6; McEnery, Xiao, and Tono 3).

While the availability of large computerized corpora has steadily increased with the power of the computers available to process them, in practice, the distinction between corpus-based and corpus-driven research, along with their rationalist and empiricist approaches, may not

be so clearly defined. While it is claimed that corpus-driven research begins free from theory, researchers must choose in advance the corpus they want to work with, along with the types of questions they may want to ask. In linguistics, this type of preliminary, instinctual knowledge about language is known as 'intuition' (Adolphs 6; McEnery, Xiao, and Tono 6), and it affects every stage of the research, from questions, to analysis, to interpretation. It is for this reason that researchers involved in electronic text analysis must make explicit the design of their corpora, their research methodology, and the identifiable theories underlying their work.

Here we return to the concept of text analysis, or 'sense making', in the words of McKee (16). If the explication of theory is key in all stages of electronic text analysis, but the task of the research is seen as fundamentally empiricist, we must ask the question: "Can we evaluate corpus evidence in the same way as we evaluate a text" (Tognini-Bonelli 2)? To rephrase Tognini-Bonelli's question, is there a difference between electronic text analysis and electronic text description?

In short, the answer is yes. Texts, electronic or otherwise, do not exist in a vacuum. It is their context that gives them meaning. As McKee explains, a text cannot even be described without some implicit placement within a greater context (65). Despite the empiricist claims of the corpus-driven research methodology, data does not simply exist, it is always undergoing some form of interpretation. This begins with the questions that are asked of the corpus, continues in the reporting of the quantitative results of its analysis, and ends in the discussion that follows (Adolphs 6; McEnery, Xiao, and Tono 9). As the philosopher of science Kuhn wrote, "more than one theoretical construction can always be placed upon a given collection of data" (Kuhn 76).

Rather than treating corpus-driven research as an endpoint in linguistic research, it should rather be considered as a means of entry, or as Adolphs describes, "a way into the data that is informed the by the data itself" (19).

A corpus is a tool for researchers that consists of a balanced, authentic and representative sample of language, situated within an identifiable context of use. It consists of text, yet it is not a 'text' so much as an object of research that can be manipulated and reorganized electronically. While corpora primarily allow for the production of quantitative data, the transmission of that data is never free from interpretation, however explicit or implicit the researcher may be about theory. It is important, as a researcher who uses corpora as a tool, to be clear about the origins, design, and use of that corpora, so that the data may be replicable and open to scrutiny. Corpora may be used for quantitative or qualitative research, often as a entry point into a larger investigation of language in use. For a mixed methods research project, the methodological path is clear: observations made as a result of the data lead to hypotheses, which lead to generalizations about phenomena, which ultimately lead to a unified theoretical statement (Tognini-Bonelli 85). The results of any research in text analysis are only as good as the corpus itself (Sinclair, *Corpus, Concordance, Collocation* 13).

The Hansard Corpus

The House of Commons debates, commonly known as Hansard, are the official edited verbatim account of the proceedings of the House of Commons (Parliament of Canada, "Debates"). The debates are published in both English and French after every sitting day, and are publicly available (Parliament of Canada, "Debates"). Transcripts have been available for download in XML format starting with the 39th Parliament on April 3, 2006. Hansard is a complete record of the proceedings of the House of Commons, recording the speeches made by MPs in debate (Parliament of Canada, "Debates"). The transcripts also contain voting lists, written answers to questions, the text from the Speech from the Throne, as well as texts of addresses from foreign dignitaries (Parliament of Canada, "Debates").

41st Parliament	
2nd	October 16, 2013 - August 2, 2015
1st	June 2, 2011 - September 13, 2013
40th Parliament	
3rd	March 3, 2010 - March 26, 2011
2nd	January 26, 2009 - December 30, 2009
1st	November 18, 2008 - December 4, 2008
39th Parliament	
2nd	October 16, 2007 - September 7, 2008
1st	April 3, 2006 - September 14, 2007

Table 3-1: Sessions of Parliament by date

The Hansard corpus used in this study has a total of 68,194,945 words. This includes all of the transcripts that comprise the 39th to the 41st Parliaments, which cover the period between April 3, 2006 and August 2, 2015.

The corpus has been split into two distinct types of groupings. The first grouping divides the corpus based on year, beginning with the year 2006 up to and including 2015. The second divides the corpus by Sessions of Parliament spanning the 39th to the 41st, as shown in Table 3-1 (Library of Parliament, "Parliaments"). This makes Hansard a diachronic monitor corpus; the corpus grows in size every time a new debate is held, and changes in the language used in the corpus can be observed over time.

The only pre-processing applied to the Hansard corpus involved the removal of the XML markup to create a raw text file. Figure 3-1 shows a sample of the Hansard corpus with XML markup and Figure 3-2 shows the same sample of the Hansard Corpus with the XML markup removed (*Hansard Vol. 147 No. 80,* 4899). The XML tags were removed in order to facilitate an accurate calculation of word frequencies and to provide readable concordances. Were a different kind of analysis required, the XML markup could easily be accessed. The raw corpus data is stored in the original XML format; the processed text is merely a copy of the data. This is truly the benefit of the electronic processing of text. Large amounts of data can be manipulated while maintaining the structure and format of the original copies.

While the Hansard corpus technically consists of spoken rather than written language, there is some uncertainty surrounding this distinction. As Mollin highlights in her study of the British Hansard, these kind of Parliamentary debates are more of a hybrid combination of

```
</ParaText>
                <ParaText id="3694786">Mr. Speaker, I would like to begin by
stating that I will be sharing my time with my colleague from <Affiliation
DbId="170184" Type="2">Timmins–James Bay</Affiliation>. </ParaText>
                 <ParaText id="3694787">I am very pleased today to move this
motion to ensure that justice is served for Canadians. However, I am very
disappointed to have to rise once again to protest this government's extremely
reprehensible actions.</ParaText>
               <ParaText id="3694788">I would have thought that, after three
years, it would have finally understood. However, once again, the government
has been caught spying on its own people.</ParaText>
```

Figure 3-1: Sample of the Hansard corpus with XML markup

spoken and written text (189). British Hansard transcripts are highly edited: repetitive speech, incomplete utterances, pauses, false starts and reformulations are omitted by the transcribers or editing staff (Mollin 189; Slembrouck 104). While no comprehensive study of the editing practices of the Canadian Hansard has been conducted, it can only be assumed by skimming the text that these characteristics have similarly been removed. For these reasons, the Hansard corpus may not be an appropriate choice for the study of spoken language, though, as Mollin concedes, the analyses of content words, much like the purpose of this study, are likely not affected by the editorial changes (189).

The Hansard corpus was chosen for its availability, consistency, size, and scope. The transcripts are posted in a timely manner and share a consistent formatting scheme. The added benefit of the Hansard corpus is that is readily available for download on the House of Commons website. Not only can other researchers access the data and replicate the text analyses, but the corpus is never in a great danger of being lost due to its constant and public availability. The regularity of sittings allows for a sufficiently large corpus, which is of the utmost importance for this type of text analysis research, especially in the development and testing of context-specific theories of language use (Bayley 34). The corpus only contains transcripts of the proceedings of the debates in the House of Commons. The Hansard corpus

```
     Mr. Speaker, I would like to begin by stating that I will be sharing my
time with my colleague from Timmins–James Bay.
           I am very pleased today to move this motion to ensure that justice
is served for Canadians. However, I am very disappointed to have to rise once
again to protest this government's extremely reprehensible actions.
               I would have thought that, after three years, it would have
finally understood. However, once again, the government has been caught spying
on its own people.
```

Figure 3-2: Sample of the Hansard corpus with XML markup removed

represents the language used by the MPs and provides a complete record of the political history in the context of the issues debated in the House of Commons. For this reason, it is an appropriate corpus with which to study the frequency and meaning of the term ‘privacy’ within Canadian political discourse.

3.2 Word Frequencies

Word frequency is a method of text analysis that refers to the numeric count of the words that are present in a corpus. The determination of word frequencies are perhaps the most direct statistical data a corpus can provide (McEnery, Xiao, and Tono 52). The frequency count of every word (or selection of words) present in a corpus is known as the 'observed absolute' or the raw frequency; it is a whole number that is greater than or equal to zero (Gries, "Statistics" 269). While this data does not provide a lot of information in terms of proving the validity of a hypothesis or claim (McEnery, Xiao and Tono 52), it does help to frame a corpus in terms of the context of language use (Adolphs 40), especially when examining the occurrence of a specific word or words. The production of these statistics is generally the first stage in any research project involving electronic text analysis (Sinclair, *Trust the Text* 28).

Once the observed absolute (raw) frequency of the words in a corpus has been generated, other types of related statistics can be produced. One method involves determining the observed relative frequency, which is the raw number of one word in the corpus divided by the total number of words in the corpus (Gries, "Statistics" 270). For example, if a corpus has 100 total words, and there are 10 occurrences of the word 'book', the relative frequency of 'book' would be 10/100 = 0.1, or 10%.

Another statistical measure that can be determined using word frequency is a type-token ratio. The analysis of this ratio can be useful when determining the level of complexity in a corpus, especially when used to compare corpora against each other (Adolphs 39). Each individual occurrence of a word is known as a token, while each unique word is called a type (Adolphs 39). Consider the following sentences:

> "There are many books in the library. Some of the books are for children, but most of the books are for adults."

Processing the above sentences in terms of their frequency would result in the following lists:

> ('there', 'are', 'many', 'books', 'in', 'the', 'library', 'some', 'of', 'the', 'books', 'are', 'for', 'children', 'but', 'most', 'of', 'the', 'books', 'are', 'for', 'adults') = 22 tokens

> ('there', 'are', 'many', 'books', 'in', 'the', 'library', 'some', 'of', 'for', 'children', 'but', 'most', 'adults') = 14 types

Dividing the number of types by the number of tokens results in the type-token ratio. In this example the calculation is 14/22 = 0.64, or 64%. Higher ratios mean more variability in terms of language use (McEnery and Hardie 50). Large corpora tend to have very low type-token ratios, not because of the simplicity of the language, but because of the preponderance of high frequency grammatical words like *the* and *to* (see Figure 3-3); in this case it is more accurate to use a sampling method to calculate the ratio, such as taking a measurement of the first 2000 words, and each 2000 words thereafter, and then calculating the mean (Baker 52).

While word frequency statistics can provide valuable insights about the nature of a corpus, when it comes to making comparisons between corpora, the validity of the data is dependent on the overall size of what is being compared (Adolphs 40). In other words, it is advisable to only make comparisons between corpora of similar lengths. If corpora of uneven lengths must be compared, the resulting data should be normalized, which means it must be adjusted to account for the size difference (McEnery, Xiao, and Tono 52).

Another important consideration is the distribution of the words under investigation in the corpus (Baker 49; Gries, "Statistics" 272). While relative frequency statistics are valuable indicators of word use, it is important to determine the distribution of relative frequencies in order to see if the words under investigation are frequent simply because they are concentrated in one area, or if they occur across the corpus as a whole (Gries, "Statistics 272).

The investigation of the frequencies of word use in a corpus, at a deeper level, is an investigation of language in context (Baker 49; Tognini-Bonelli 87). The observation of cumulative patterns of repeated word use allows for the interpretation of a body of text in a way that is not possible by reading or listening alone. While the output of a word frequency analysis may be purely statistical, according to Burrows, the study of the words themselves uncovers the "underlying fabric of a text, a barely visible web that gives shape to whatever is being said" ("Textual Analysis").

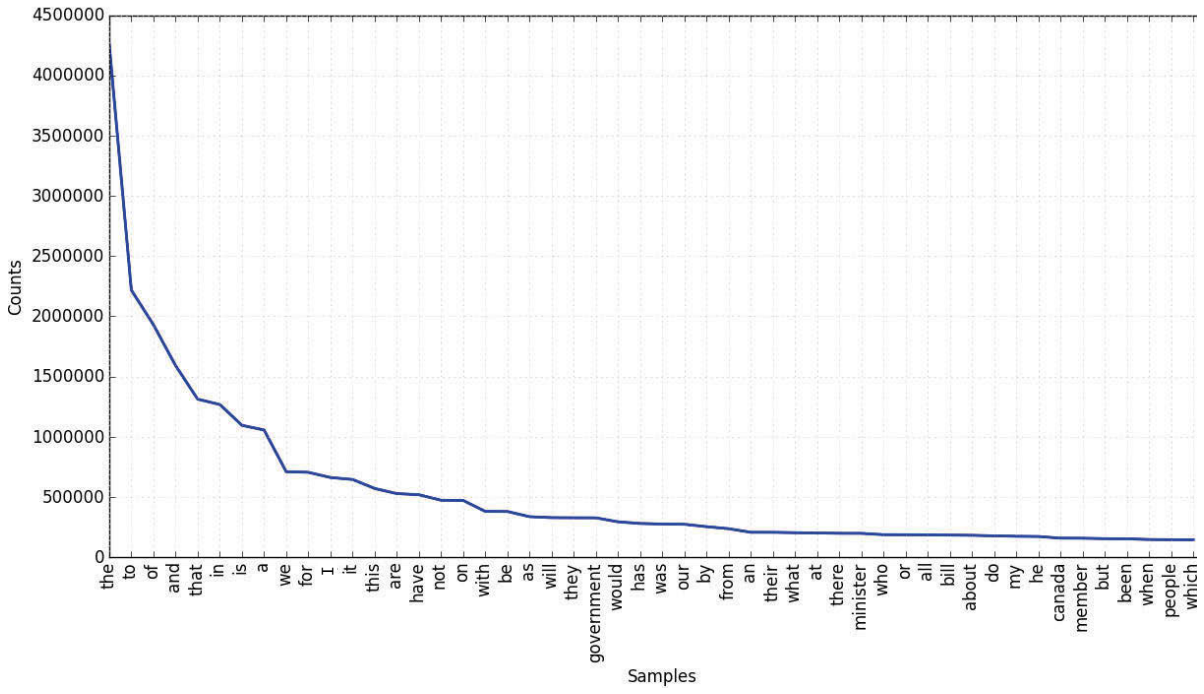

Figure 3-3: Frequency of the top 50 words in the Hansard corpus

The Hansard Frequencies

The distribution and frequency of words in texts is incredibly uneven due to two broad categories of words found in the English language: content words and function words (Stubbs, *Words and Phrases* 39). Content words describe what the text is about, while function words

Year / Parliament	Raw Frequency	Ratio %
2006	356	0.007
2007	258	0.004
2008	252	0.005
2009	612	0.009
2010	533	0.009
2011	624	0.012
2012	552	0.008
2013	918	0.015
2014	1567	0.022
2015	806	0.020
39-1	538	0.006
39-2	308	0.005
40-1	20	0.004
40-2	612	0.009
40-3	1011	0.013
41-1	1287	0.008
41-2	2702	0.021

Table 3-2: Raw and relative frequency of the word 'privacy'

help tie the content words together (Stubbs, *Words and Phrases* 39). The Hansard corpus is no different. Figure 3-3 shows the frequency of the top 50 words in the entire corpus.

The word 'the' appears over 400,000 times in the Hansard corpus, which is almost twice as many times as the second most frequent word: 'to'. The word under investigation in this study, 'privacy', has a total raw frequency of 6,478, while the relative frequency or ratio is 0.011%. While this is a fairly insignificant number in itself, the dispersion statistics provide more context.

Table 3-2 shows the raw and relative frequency of the word 'privacy' in the Hansard corpus. Between the years 2006 and 2015, as well as between the 39th and 41st Parliaments, there is an observable trend of increased usage of the word. This is especially apparent between the years 2013 and 2014, and between the first and second session of the 41st Parliament. The data from 2014 is especially compelling, because the relative frequency is the highest in that period compared to any other year or Session, which makes 2014 worthy of further investigation. Despite a few anomalies, there is an overall positive trend of the instances of the word privacy between 2006 and 2015, and between the 39th and 41st Parliaments.

Examining the raw and relative frequencies also illuminates how misleading it can be to rely on raw frequency alone. While the raw frequency in 2009 and 2011 are within 12 words of each other, the relative frequency for 2011 shows a higher percentage of relative use. This is also clearly illustrated by the frequencies in 39-2 and 40-1. While there seems to be a drastic reduction in raw frequency between the two sessions, the relative frequency differs only slightly. This is

Year / Parliament	Raw Frequency	Ratio %
2006	22	0.00042
2007	9	0.00015
2008	0	0.0
2009	50	0.00074
2010	29	0.00046
2011	72	0.00133
2012	47	0.00066
2013	46	0.00074
2014	101	0.00144
2015	35	0.00088
39-1	30	0.00032
39-2	1	0.00002
40-1	0	0.0
40-2	50	0.00074
40-3	98	0.00124
41-1	90	0.00059
41-2	142	0.00111

Table 3-3: Raw and relative frequency of the phrase 'privacy rights'

Year / Parliament	Raw Frequency	Ratio %
2006	5	0.00010
2007	6	0.00010
2008	2	0.00004
2009	11	0.00016
2010	19	0.00030
2011	44	0.00081
2012	20	0.00028
2013	42	0.00068
2014	30	0.00043
2015	15	0.00038
39-1	9	0.00010
39-2	4	0.00006
40-1	0	0.0
40-2	11	0.00016
40-3	60	0.00076
41-1	59	0.00038
41-2	51	0.00040

Table 3-4: Raw and relative frequency of the phrase 'right to privacy'

Both 'right to privacy' and 'privacy rights' are represented with a significant relative frequency in 2011. This same pattern exists in the 3rd session of the 40th Parliament. Since that session took place during the first three months of 2011, it can be deduced that there was a substantial amount of discourse concerning privacy rights in the House of Commons between January and March of that year.

The phrase 'privacy rights' shows another significant increase in frequency in 2014, though 'right to privacy' does not. This is echoed in the high frequency for 'privacy rights' in the 2nd session of the 41st Parliament.

The phrase 'reasonable expectation of privacy' shows a substantial increase in relative frequency starting 2013 and continuing through 2015. A dramatic increase in relative frequency is also shown in the 2nd session of the 41st due to the fact that significantly less words were spoken in 40-1 overall.

In the last chapter, the concept of privacy rights and the meaning of 'reasonable expectation of privacy' was discussed at length. After conducting the concordance analysis described in the upcoming section, a trend was discovered connecting the word 'privacy' with 'rights', both as 'privacy rights' and 'right to privacy'.

The frequency of these phrases, as well as the phrase 'reasonable expectation of privacy' is of interest to this investigation. Table 3-3, Table 3-4, and Table 3-5 show the raw and relative frequencies for each of these phrases.

Year / Parliament	Raw Frequency	Ratio %
2006	0	0.0
2007	0	0.0
2008	0	0.0
2009	3	0.000044
2010	2	0.000032
2011	0	0.0
2012	1	0.000014
2013	6	0.000097
2014	13	0.000185
2015	10	0.000251
39-1	0	0.0
39-2	0	0.0
40-1	0	0.0
40-2	3	0.000044
40-3	2	0.000025
41-1	3	0.000020
41-2	27	0.000211

Table 3-5: Raw and relative frequency of the phrase 'reasonable expectation of privacy'

Parliament, which began in October of 2013. Again, it is clear that a specific discourse concerning the topic of a 'reasonable expectation of privacy' was conducted in the House of Commons during this time frame.

Clearly the raw and relative frequencies for 'privacy' and its related phrases are all quite low, given that the total number of words in the corpus is almost 69 million. But regardless of numbers, an examination of raw and relative frequencies show areas of the corpus that merit additional analysis. This is a clear example of the way in which corpus data can pinpoint areas of interest for further research.

The manual examination of 69 million words, comprising tens of thousands of pages of text, would be an incredibly time consuming task. The conclusive discovery of trends in the specific use of a word or phrase over an eight-year period would be practically impossible to achieve by just reading the text alone.

The results of these frequency statistics will be further supported by the next section on concordances, though these frequency results stand for themselves in terms of narrowing the field of focus for a closer and more detailed analysis of the Hansard corpus.

3.3 Concordances

A concordance is another method of electronic text analysis. Concordances serve the purpose of bringing together, or concording, passages of text that help to show how a word is used in context (Howard-Hill 4). Concordance outputs are not limited to whole words, they can also be tailored to show lists of letters, phrases, suffixes, and parts of speech (nouns, verbs, etc.) (Adolphs 5; McEnery and Hardie 35).

The most common format for a concordance is known as a Key Word in Context, or KWIC, and it is arranged so that all instances of a search item are in the middle of the page (Adolphs 52; Baker 71; Tognini-Bonelli 13). This search item is often referred to as a 'node', and all of the words on the left and right of the node are called the 'span'. Descriptions of concordance data label the node as N, and the items on the sides as N-1, N-2, N+1, N+2, etc. (Adolphs 52), depending on their distance and position in relation to the node. Figure 3-4 is an example of a KWIC generated from the Hansard corpus where N = privacy.

```
Displaying 25 of 918 matches:
 1 imply unacceptable. That is why the Privacy Commissioner's office was notified.
 2  the matter to the attention of the Privacy Commissioner of Canada. I also aske
 3 table. That is why we called in the Privacy Commissioner and called in the RCMP
 4 able. That is why we brought in the Privacy Commissioner. That is why we brough
 5 ese victims and when will they take privacy protection seriously? (1455) Hon. D
 6  is why we took steps to inform the Privacy Commissioner of Canada and to bring
 7 ystems to make sure that Canadians' privacy is protected. That is why we have e
 8  happened. We have also advised the Privacy Commissioner of the situation. We h
 9 . Speaker, the government takes the privacy of Canadians extremely seriously. T
10 ely unacceptable. The Office of the Privacy Commissioner has been notified and
11 nment takes extremely seriously the privacy of Canadians and the loss by the de
12 ion. We will continue to do so. The privacy commissioner is investigating this.
13 ed before, the government takes the privacy of Canadians extremely seriously- S
14 mentioned, the government takes the privacy of Canadians extremely seriously. T
15 p greater chances for fraud. As the Privacy Commissioner now conducts her inves
16 g Bob Zimmer Access to Information, Privacy and Ethics Chair: Pierre-Luc Dussea
17 stioned Conservative legislation on privacy concerns, we were accused of standi
18 006. According to the Office of the Privacy Commissioner, this is one of the la
19 he Information Commissioner and the Privacy Commissioner. I will try to delinea
20 the Information Commissioner or the Privacy Commissioner. Each of them are offi
21 ve seen the value of an independent Privacy Commissioner working on behalf of a
22 a government agency. Canada's first Privacy Commissioner, Inger Hansen, was wit
23 ssion at first, and then, under the Privacy Act, became an independent officer
24 tion Commissioner, Auditor General, Privacy Commissioner, we say the Parliament
25 neral, Information Commissioner and Privacy Commissioner are all examples of of
```

Figure 3-4: Selection of 25 random concordance lines

Just above the KWIC is a line stating that this particular list contains 25 instances out of a total of 918 matches. This means that the concordance program found a word frequency count for 'privacy' totaling 918 occurrences in this search. The node word, privacy, is found in the centre of the page and the total sentence span is equal to 79 characters (including letters, punctuation and spaces).

It is immediately apparent the potential that concordance outputs have for the generation of hypotheses about corpora (Adolphs 51). The nature of the concordance format provides a convenient layout for examining word or phrase use in context, along with the identification of trends or patterns in language use (Stubbs, *Text and Corpus Analysis* xviii). The example in Figure 3-4 shows 16 occurrences of the word 'privacy' in relation to the word 'Commissioner', one instance of the phrase 'Privacy Act', and one instance of the phrase 'Access to Information, Privacy and Ethics Chair'. Of the remaining seven instances, when the words to the right of the node are examined, four include the phrase 'privacy of Canadians', two include the lemma 'protect', and the remaining instance contains the word 'concern'. A lemma is a base-word from which other words can be constructed, even though they may differ in form or spelling (Baker, Hardie and McEnery 104; Sinclair, *Corpus, Concordance, Collocation* 41). 'Protection',

```
 1  stioned Conservative legislation on privacy concerns, we were accused of standi
 2  are specifically intended to reduce privacy concerns and to increase accountabi
 3   identifying information because of privacy concerns. However, some files dealt
 4  f law and strikes a balance between privacy concerns and investigations that ca
 5  of the victims clearly outweigh the privacy concerns for the offenders. Bill C-
 6  the government plans to address the privacy concerns of Canadians who have been
 7  ringe on civil liberties. It raises privacy concerns that ought to be referred
 8   Act. This would be just to protect privacy concerns of people who may have bee
 9  DA allows for mediated solutions to privacy conflicts that can give both indivi
10   verify that operational, legal and privacy considerations are met. With regard
11   supposed to be protecting personal privacy data, but we see that is creating a
12 fear they have been hacked and that privacy data has been breached, it has to b
13 as once seen as the world leader in privacy data. Our Privacy Commissioner is d
14 ment seems to think that losing the privacy data of one million Canadian senior
15 powers and the authority to protect privacy data from hacking, how does she com
16  which is address the protection of privacy data in the age of big data, with t
17 ith the NDP to protect the right to privacy declared victory yesterday when Bil
18  that this bill follows the court's privacy directives. Some of the bill's word
19 at avoids litigation when resolving privacy disputes. PIPEDA also provides the
20 arding individuals is a significant privacy enhancement. This dual approach wil
21  hear from civil society groups and privacy experts and other jurisdictions whe
22 were repeated calls by Internet and privacy experts and civil society groups to
23  only from civil society groups and privacy experts but from those familiar wit
24  There have been concerns raised by privacy experts, by digital experts, that t
25 ns, in particular legal experts and privacy experts, raising concerns with the
```

Figure 3-5: Selection of 25 concordance lines sorted alphabetically at N+1

and ‘protected’ are both variations on the lemma ‘protect’.

While concordances can be investigated manually in this manner, they can also be rearranged alphabetically on either side of the node. Figure 3-5 shows a sample of right node alphabetization. The concordance can be further sorted based on a selective number of objective criteria (Tognini-Bonelli 13). Using Figure 3-4 as an example, all of the lines containing the phrase ‘Privacy Commissioner’ have been filtered out as they were deemed unnecessary to this particular analysis. Alternatively, adding a second word to the concordance search (within a span of one or two words) can help identify particular themes of usage (Adolphs 55).

History

While computers make the production of concordances much easier, their history pre-dates the electronic age. Early concordance work was produced with the intention of studying quotations, allusions and figures of speech in literature, not everyday language (Sinclair, *Corpus, Concordance, Collocation* 42). What is considered to be the first concordance was hand-compiled for the Latin Vulgate Bible by Hugh of St Cher with the assistance of over five hundred monks in 1230 (McEnery and Hardie 37). Father Roberta Busa compiled the first automated concordance, a project which began in 1951 (Hockey; McEnery and Hardie 37), and by the 1960’s scholars were beginning to see the value of concordances for the purpose of textual and literary analysis. The first generation of concordancers were held on large mainframe computers and used at a single site (McEnery and Hardie 37). They were generally only able to process non-accented characters from the Roman alphabet; accented characters would be replaced by a pre-determined sequence of characters, although these were not standardized and differed from site to site (Hockey; McEnery and Hardie 38). Early concordancers also had difficulty locating the exact location of the citations in the text, as the raw textual information was stored on punch cards or tape. Variant spellings of words and the production of lemmatized lists were also problematic (Hockey).

The nature of the programming involved to create concordance outputs at this time required the assistance of a computer programmer or engineer, something that was not accessible to all scholars (McEnery and Hardie 38). The second-generation of concordancers solved this issue, as they were available as software packages on IBM-compatible PCs (McEnery and Hardie 39). While these concordance programs suffered from many of the same limitations as earlier concordancers, they made electronic text analysis more accessible (McEnery and Hardie 39). Since the inception of automated concordancing in the 60s, the methods, accessibility and scope has drastically improved. Currently, concordance programs exist as downloadable software, web-based applications, and packages of pre-made code for those interested in computer programming.

Theory

While the production of concordance outputs is essentially another method in the practice of electronic text analysis, this does not mean the technique is one of complete objectivity. Corpus data is not an ontological reality; it is constructed and delimited by the researcher in an attempt to gather meanings about the discourse under study (Teubert 4). In other words, although the corpus exists and is tangible in many ways, it is not a stand-in for the reality of

the Parliament. It is a representation of reality that takes its own form and becomes an object in and of itself. Concordances provide the opportunity to examine language in context, and the structured nature of the output helps to ensure that analysts do more than pick examples that meet their preconceptions of the data (Stubbs, *Text and Corpus Analysis* 154). Yet the theoretical intention of the researcher is still present at every stage, from search choice to interpretation (Stubbs, *Text and Corpus Analysis* 154). What concordance outputs provide is the ability to present quantitative evidence of electronic text analysis that can be examined by all readers (Stubbs, *Text and Corpus Analysis* 154).

Concordances are what Stubbs refers to as "second-order data" (*Words and Phrases* 66). First-order data is the corpus, or what can be called the 'raw data'; this data is too large for accurate observation and analysis, leading to the creation of second-order data, which is comprised of the word frequencies and concordance output (Stubbs, *Words and Phrases* 66). A large corpus generates a large amount of concordance lines, and although these can be managed through sampling, further statistical processing can be done to create what Stubbs calls third-order data, which are known as collocates (Stubbs, *Words and Phrases* 67).

Words in the English language have a tendency to appear with other words (Stubbs, *Words and Phrases* 17), giving phrases or groups of words a meaning that transcends the value of each individual word if considered separately (Sinclair, *Corpus, Concordance, Collocation* 104). Collocates are words that co-occur with other words, and lists of these words can be generated algorithmically, accompanied by statistics that determine their significance (Stubbs, *Words and Phrases* 29).

In terms of this research, collocational statistics were generated but not used, simply because they did not provide any compelling or new evidence to support what had already been discovered through the frequency and concordance analysis. Notably, both Danielsson (112) and Wermter and Hahn (791) have come to the same conclusion regarding the usefulness of collocational data, arguing that frequency statistics alone provide strong enough evidence to support claims about language use.

The Hansard Concordances

A corpus as large as Hansard does not allow for the inspection of every concordance line, and there are many instances that are not worthy of inspection, such as the multiple instances of "Privacy Commissioner" in Figure 3-4. Sampling and alphabetical sorting make the manual inspection of concordance outputs easier and more efficient. That being said, Sinclair makes a valid point in saying that regardless of the thoroughness of the study, there will always be data left over to perform an even more comprehensive study (*Corpus, Concordance, Collocation* 65). Concordance analysis, much like word frequency calculation, has the purpose of identifying patterns of interest in the corpus that can be highlighted for further study.

Sampling

A preliminary method of reviewing concordance output consists of simply scanning down the list and noting any observable patterns. The concordances are produced in order, which in a sense, becomes a timeline of the node word as it has been used in the corpus from the

beginning to the end of the measurement period.

When faced with a large corpus such as Hansard, Sinclair suggests a methodical sampling method to make the analysis more manageable. This involves dividing the number of instances of the word by the number of concordance lines desired, using 25 concordance lines as a general standard (Sinclair, *Reading Concordances* xviii). For example, if there are 5000 instances of a word and 25 concordance are lines required, then 5000 is divided by 25 for a total of 200. This total is the gap between selections, meaning that 25 lines from every 200 lines should be sampled. Starting at concordance line no. 1, the first 25 concordance lines are selected, then lines 201 through 225, then 401 through 425 and so on until the last instance, in this example, no. 4801 (Sinclair, *Reading Concordances* xviii). The Hansard corpus was sorted in this manner, both by year and by Session of Parliament. This resulted in groups of seven to 18 concordance samples for each year, and 14 to 21 samples for each Parliament (depending, of course, on the frequency of 'privacy' for each section). Each concordance sample contained 25 lines.

Alphabetical Sorting

Once the samples were generated, the resulting concordance lines were sorted alphabetically. The lines were sorted on the right node at position N+1, the first word to the right of 'privacy', see Figure 3-5 for an example of this type of sorting. This position yielded the highest amount of duplicate lines for omission, those lines being: Privacy Act; Privacy Commissioner; and Access to Information, Privacy and Ethics. The concordance lines containing those phrases were omitted because they did not accurately represent the pattern of the use of the word 'privacy' as a means of determining its meaning. Each sample was then examined to determine any thematic patterns of word use.

sexual images of themselves in the privacy of their own home for their own per
some other country determining the privacy of my personal information. It then
f their own home or a doctor in the privacy of their own doctor's office. Only

Figure 3-6: Selection of concordance lines with a 'personal' context

isadvantage because it respects the privacy of veterans and their families. One
to do their job and protecting the privacy of law-abiding Canadians. Everyone
t out that those same hunters whose privacy the government wants to protect als

Figure 3-7: Selection of concordance lines about 'privacy and people'

an while respecting the charter and privacy rights of Canadians. I also believe
n the civil liberties and rights to privacy of Canadians by passing information
t is trying to roll back Canadians' privacy rights is not constitutional. Does

Figure 3-8: Selection of concordance lines about 'privacy and rights'

Positive context

line rules for business. Protecting privacy is good for Canadians, good for bus
n the bill that we think strengthen privacy protection for Canadians, including

Negative context

s a remarkable breach of Canadians' privacy by their own government. Not only w
h as FATCA, which could violate the privacy of thousands—if not tens of thousan

Figure 3-9: Selection of concordance lines with a 'positive' or 'negative' context

Interpretation

Answering the research question asked of this section, the concordance output from the Hansard corpus identified the following patterns regarding the use of the word 'privacy': privacy is something personal and can imply ownership, information, or space (Figure 3-6); privacy affects certain groups of people, including Canadians, veterans, taxpayers, children, travelers, women, hunters, and law-abiding citizens (Figure 3-7); and privacy has something to do with rights, in the context of human rights, civil rights, constitutional rights, the Charter, and freedom of speech (Figure 3-8).

Grammatically, privacy is something that can be referenced in a negative or a positive light, and these phrases consist most commonly of verbs like breach and violate, or protect and strengthen (Figure 3-9); and privacy is often used as the first word in a phrase with nouns, such as 'privacy interests' or privacy obligations' (Figure 3-10).

t talk to people? There are serious privacy interests at stake, as well as the
as to where Joe Smith works, due to privacy situations. However, we can certain
. The first item is, do we know our privacy obligations? Some businesses are bu
nging for us to understand the full privacy implications of Bill C-11, such as

Figure 3-10: Selection of concordance lines with 'privacy' as a phrase

While there were certainly outliers in the samples collected, including phrases like "privacy on the other hand" or "privacy screen", the overwhelming majority of examples fell into one or more of the previous categories.

Key Observation

In terms of the specific phrases identified in the previous section on frequency calculations, a closer look at the phrase 'privacy rights' shows that it is often used in conjunction with the phrase 'Canadians', or more interestingly, 'law-abiding Canadians' (shown in Figure 3-11). As it was discussed in Chapter 2, 'privacy rights' is not necessarily an accurate term, as there is no specific right to privacy in Canada. The connection between 'privacy rights' and 'law-abiding Canadians' is especially interesting, given that the judgment in *R. v. Spencer* ruled that privacy protections apply to all Canadians, even when they've clearly broken the law.

gling. I assure the member that the privacy rights of law-abiding Canadians are
r, I can assure the member that the privacy rights of law-abiding Canadians are
blic Safety, CPC): Mr. Speaker, the privacy rights of law-abiding Canadians are
ers. The minister claimed that “the privacy rights of law-abiding Canadians are
something. This motion defends the privacy rights of law-abiding Canadians, an
ocrats do not support violating the privacy rights of law-abiding Canadians. Wh

Figure 3-11: Selection of concordance lines with the phrase 'law-abiding Canadians'

Again, while it is hard to speculate on specific reasons for these trends without investigating the corpus more thoroughly, the concordance data provides yet another layer upon which to focus the investigation in the next chapter.

3.4 Results

This chapter used text analysis to investigate the transcripts of the debates in the House of Commons in order to uncover the meaning of the word 'privacy'.

The investigation determined that the utterances of 'privacy' increased in frequency during the sample period, from a total of 0.007% of the total words spoken in 2006 to 0.020% in 2015. The analysis of the concordance data, in tandem with the frequency analysis, uncovered the ways in which 'privacy' was used in debates, leading to a clarification of the meaning of the term as it is used in Parliamentary discourse. The text analysis showed an increasing trend of phrases describing 'privacy' as a 'right' held by individuals and groups, and that this 'privacy right' is in need of protection and respect in order to prevent breaches and violations.

More specifically, the frequency data revealed a interesting trend regarding the phrase 'privacy rights'. In 2011, especially during the months of January to March inclusive, 'privacy rights' has the highest relative frequency compared to all of the preceding years. Upon further examination of the concordance data from this specific period, the connotation of the words used in proximity to this phrase was more negative in tone than positive. This trend is not confined to 2011, but includes the entire 3rd session of the 40th Parliament. Interestingly, in 2014, when the phrase shows a further increase in relative frequency, the analysis of the concordance data shows the opposite trend. Words used in proximity to the phrase 'privacy rights' tend to be more positive in tone than negative.

It could be argued that this positive trend is not positive at all, as the relationship between 'privacy' and words such as 'protect' or 'respect' may actually imply a current state of vulnerability or disrespect that needs changing. Alternatively, words like 'breach' and 'violate' may actually be positive, as their use may imply that privacy is being protected, rather than threatened. For this reason, these trends will not be investigated further in the scope of this thesis.

Parliamentary discourse, and the subsequent creation of laws, establishes what may or may not be done in a given society (Bayley 12). The text analysis research in this chapter has revealed that privacy is continuously described as a 'right' in the House of Commons, with the use of phrases such as 'right to privacy' and 'privacy rights'. Despite this discourse, there exists no actual right to privacy in Canada, but only the quasi-constitutional right to the protection of personal information held for federal or commercial purposes, where a reasonable expectation of privacy exists. As discussed in the last chapter, this does not constitute an actual right to privacy, despite how it is discussed and debated by Members of Parliament.

This contradiction merits a further investigation of the discourse of privacy in the House of Commons. Why do Members of Parliament consistently refer to privacy as a 'right' when the reality of 'privacy rights' in Canada are subject to continuous interpretation by the courts, as well as a lack of a substantive definition of privacy in the legislation? Why are some of the instances of 'privacy' and 'privacy rights' modified with the addition of the phrase 'law-abiding Canadians'?

While the results of the text analysis highlighted the reoccurring trends and patterns of language at the level of the word, phrase, and sentence in the Hansard corpus, the Critical Discourse Analysis in the next chapter will focus on an examination of language-in-use, and the ways in which the discourse of privacy can shape the expectations of the meaning of the word itself.

4 Critical Discourse Analysis

Following the 'distant reading' of Hansard in the last chapter, the purpose of this chapter is to conduct a 'close reading' of a specific debate in the House of Commons. Using the method of Critical Discourse Analysis, this stage of the research will bring meaning to the data collected in the first text analysis by uncovering and contextualizing the observed patterns and trends of language used by MPs.

Discourse analysis explicitly studies language in use (Taylor 5). Though language is not the same as discourse, it is fundamental to its production and interpretation (Baker 5). A discourse is an authentic text that performs a social function (Mautner 123-124) and provides a representational view of language (Fairclough, *Language and Power* 7).

Text, as it was described in the last chapter, includes both spoken and written language (Stubbs, *Words and Phrases* 5). Texts are not only produced, but consumed by individuals in society, and this consumption is dependent on a process of interpretation that draws on the individual's prior knowledge of language, as well as their own values and beliefs (Fairclough, *Language and Power* 57). This process of interpretation then serves to inform the subsequent production of individual's own texts (Fairclough, *Language and Power* 57). The knowledge, values, and beliefs of individuals (which can be referred to collectively as cognition), do not exist in a vacuum, they are socially generated through the experience of 'being' in society (Fairclough, *Language and Power* 57). Discourse is the result of the social context and interactions that influence and inform the interconnected processes of the production and interpretation of texts (Fairclough, *Language and Power* 57).

The purpose of discourse analysis is to uncover not just the meaning, but the intention of text, which includes the context within which it was created (McEnery and Hardie 133; Stubbs, "On Text" 145). The 'analysis' in discourse analysis can be understood as the systematic and procedural attempt to identify patterns in a text in order to link them to patterns observed in the context of its creation (Mautner 124).

Critical discourse analysis (CDA) is discourse analysis done through a critical lens. Doing analysis 'critically', according to Gerlinde Mautner, can be understood as "unveiling and challenging taken-for-granted assumptions about language and social life, as well as recognizing discourse as a potentially powerful agent in social change" (124). It is a study of how social power, abuse, dominance, and inequality are communicated, as well as reinforced or resisted, in the social and political context of discourse (Dijk, "Critical Discourse Analysis" 352). The purpose of CDA is to show the "non-obvious" ways in which language contributes to systems of power and dominance in society (Fairclough, "New Labour" 229).

Norman Fairclough, one of the founders of CDA, argues that language and society are not distinct entities, but two parts of an interrelated whole (*Language and Power* 56). Language is inherently social; the purpose of linguistic communication, whether through speech or the written word, is to interact with others in society, and these interactions are influenced by learned social conventions (Fairclough, *Language and Power* 56). The ways in which people

communicate in one aspect of society, such as within political institutions, are drastically different from the ways in which they communicate in others, such as in their own homes. Society is also, in part, inherently linguistic; social conventions of language not only mediate, but help to maintain the structure of society itself (Fairclough, *Language and Power* 56). If communicating using context-specific conventions of language, such as political debate, weren't a necessary requirement for politicians in the House of Commons, than other non-discursive elements of the institution would likely be different. For example, the absence of debate would drastically change the role of the Speaker of the House of Commons, as they are sole person responsible for enforcing and interpreting the rules and practices of parliamentary debates (O'Brian and Bosc).

In order to analyze discourse, we must analyze the social conditions within which it is created and reproduced. Fairclough describes social conditions in terms of an interconnected network of social events, practices, and institutions that comprise society as a whole (Fairclough, "New Labour" 235; Fairclough and Fairclough 328; Fairclough, *Language and Power* 57). Fairclough's method of analysis requires more than a detailed investigation of individual texts, it also involves a comprehensive interpretation and explanation of the network of social conditions that led to the its creation (Fairclough, *Language and Power* 58-59). These three stages--text analysis, interpretation, and explanation--form the methodological basis of CDA.

According to Fairclough, society is comprised of institutions that serve to divide the experience of social life into domains of experience, made up of individual situational contexts (*Language and Power* 61). Politics, as an institution in Canada, can be divided into domains consisting of city, provincial, and federal governments. Within each of these domains are specific situational contexts, like City Halls, provincial Legislatures, and Parliament.

Social practices inform the ways in which a society is structured, permeating through all layers of situational contexts, domains, and institutions, as well as across them (Fairclough, *Language and Power* 60). Social practices consist of the expected and conventional "ways of acting, ways of representing and ways of being" associated with particular social roles in society (Fairclough and Fairclough 329). These social roles, which Fairclough describes as 'subject positions', determine, through an understanding of social practices, how people are expected to act, relate, and behave in particular situational contexts (Fairclough, *Language and Power* 68). Society is comprised of many social roles, like those of politician, business person, or parent, each with their own corresponding set of social practices. These social roles and practices can overlap, compliment, or exist in opposition to each other.

Social roles and practices influence social events, which are the concrete and individual instances of things happening in the world, where actual people act, relate, and behave in specific and observable ways in specific situational contexts (Fairclough and Fairclough 328).

For example, a politician attending a meeting or signing papers in their place of work is an example of a specific social event. Meetings and paperwork are expected social practices that those in the social role of politician participate in, though people in other social roles (like those in business) may have the same kinds of practices. Politicians may also participate in

different types of practices depending the situational context they are in, such when they meet with constituents or when they are campaigning. These different types of practices become grouped together and networked in particular ways that contribute to the structure of specific institutional contexts, so that the practices that exist within one domain are understood and defined in certain ways as being distinct from the practices that exist in another. When types of social practices are grouped together this way, they constitute what Fairclough describes as social orders (*Language and Power* 61). Social orders can exist within situational contexts, domains, and institutions, but also across them. For example, in Canada, the social orders of the institutions of politics and business exist within the broader social order of democracy and capitalism.

Discourses exist within each of these social conditions, and as it was discussed earlier, they are both influenced by and exert influence on the structure of society. Discourse at the level of social events involves the production and interpretation of actual texts by individuals in society, like politicians debating a motion or speaking in political advertisements. Social practices result in types of discourse that are linguistic representations of aspects of reality, which are often identifiable by the ways that they reflect the perspectives and practices of different social roles (Fairclough and Fairclough 330; Fairclough, *Language and Power* 57). For example, political debates are recognizable in that they adhere to rule-bound conventions of language and organization, and while political advertisements don't need to follow the same rules, they have their own rules, which also may or may not apply depending on the context, such as during an election. Both practices are distinguishable from each other in identifiable ways while remaining generally recognizable as a discursive political practice.

Much like there are social orders within and across contexts, domains, and institutions, there are corresponding orders of discourse (Fairclough, *Language and Power* 61-62). Orders of discourse include the myriad and complex interplay of conventions of language; from the formal properties of language itself, to genres of communication (i.e. conversations vs. speeches), to the overall ideological content (Fairclough, *Language and Power* 61-62).

As it has been described so far, society, its constituent institutions and domains, and their resulting social and discursive practices all have a tremendous influence on the ways in which people go about their lives, but the reality of social life does not make things completely pre-determined. Social and discursive practices are reflections of reality, and while they may influence it, they do not comprise it (Fairclough, *Language and Power* 69).

In reality, people 'draw upon' orders of discourse as they relate with others and with society, but they are also influenced by their own cognition (Fairclough, *Language and Power* 69). Social roles may constrain what may be said and done, but they are not absolutely binding, meaning that people are somewhat free to be creative in the ways in which they act and interact. Fairclough describes this concept with the term 'reproduction'. The interpretation and reinterpretation of discourse, combined with individual cognition (which itself has been influenced socially), produces and reproduces discourse types to the point where they may be modified or changed completely (*Language and Power* 69). This happens as a result of the reflexive nature of cognition, in that individuals can actively examine their individual knowledge,

values, beliefs and seek to consciously change them, which can lead to the eventual shift in orders of discourse, and ultimately a change in the structure of society itself (Fairclough and Fairclough 396).

But reproduction also maintains orders of discourse, and this is precisely what makes language so powerful in society. Part of this power is reflected in the ways in which discourse can be used to prioritize certain social roles, practices, and structures over others, resulting in a system where social relationships are unequal (Fairclough, *Language and Power* 71). For example, it is understood as a matter of practice that only elected Members of Parliament may participate in debates in the House of Commons, and while other people may watch, they may not speak.

According to Fairclough, conflicting orders of discourse, which are intrinsically related to social orders, lead to the implication that some discourses are more dominant, mainstream, or 'right' than others ("New Labour" 235). This is where the concept of hegemony is particularly useful to CDA. Hegemony refers to power and power struggles, where power is obtained and maintained through consent, rather than coercion (Fairclough, "New Labour" 233). The hegemony of a dominant social order is sustained through the communication and maintenance of certain orders of discourse as being 'common sense', which in turn influences the cognition and behaviour of people in their everyday lives (Fairclough, "New Labour" 233; Fairclough, *Language and Power* 13). Fairclough's use of the term 'common sense' as a construct of hegemony is heavily influenced by Antonio Gramsci, a neo-Marxist theorist and politician who argued that the power of the ruling class is effectively exercised by the cohesive nature of the 'common sense' beliefs of people in subordinate classes (Gramsci 420). A 'common sense' belief is a "conception of the world which is uncritically absorbed by the various social and cultural environments in which the moral individuality of the average man is developed" (Gramsci 419).

Using the previous example, it seems as though disallowing anyone but MPs to participate in debates is just 'common sense', but really, it is a social practice that is sustained ideologically and maintained through the entire structure of the institution of politics. While there may be valid reasons for the practice, it is still just a practice, just one that is constantly being reproduced. This relationship between power, discourse, and common sense will be explored in more depth in the next section.

A critical discourse analysis requires more than just an examination of texts. CDA requires the analysis of the relationship between texts, the discursive process of textual production and interpretation, and the social context within which they were created. This context includes immediate situational practices of society, as well as the social structures within which the social practices and roles are enacted (Fairclough, *Language and Power* 58). Fairclough describes these three dimensions of discourse as text, interpretation, and context (*Language and Power* 58).

There are three dimensions of discourse that construct the three interconnected, but hierarchical stages of Fairclough's method of CDA: the first stage describes an actual text in

terms of its formal properties of language, such as the vocabulary and grammar; the second stage analyzes the text as a product of a social interaction, through an interpretation of the process of production and interpretation; the third stage explains the text in terms of the relationship between the social interaction it represents and the social context within which the interaction occurs (Fairclough, *Language and Power* 58-59, 129).

The purpose of CDA is to uncover the social conditions that contribute to the creation of discourse by uncovering the ways in which language influences the ideological relations of dominance and power in society (Fairclough, "New Labour" 231; Fairclough, *Language and Power* 7). The critical nature of CDA is more than the act of identifying discourses that are open to critique, such as those that are false or misleading, but asking why the discourse exists in the first place (Fairclough, *Language and Power* 7). The reason for such a critique is to provide an explanation that becomes the basis for action that can advocate for change in particular aspects of the social reality under analysis (Fairclough, *Language and Powe*r 6-7).

When CDA is applied to political discourse, it can be called political discourse analysis (PDA). This type of analysis, under the broader umbrella of CDA, deals specifically with the "reproduction of political power, power abuse, or domination" found in political discourse (Dijk, "Political Discourse Analysis" 11). What defines the discourse as 'political' in this chapter are the texts, interactions, and context under examination: the texts are the transcripts of Hansard, and the interactions involve Members of Parliament engaging in the discursive political practice of debate in the situational context of the House of Commons, which itself exists within the context of a system of parliamentary democracy.

Purpose of this Chapter

This chapter will use the methodology of CDA to examine and critique the political discourse in the House of Commons, specifically on the topic of privacy. Although aspects of privacy are protected by law in Canada, privacy is not included as a specific right in the Charter of Rights and Freedoms. This legislative reality is in opposition to the results of the text analysis in the last chapter, which showed an increasing trend involving the use of the phrase 'privacy rights' in Hansard between the 39th to the 41st Parliaments, with the most prevalent use occurring in the 3rd Sess. of the 41st Parl., Specifically during the year 2014.

Research Question

Using the trends identified by the text analysis along with the understanding of the current state of privacy legislation in Canada, this chapter will use methodology of CDA to investigate the following question:

- Why do Members of Parliament consistently refer to privacy as a right when the reality of privacy legislation in Canada is limited to the protection of specific aspects of personal information in limited domains?

It is important to point out that the subsequent analysis of the political discourse of privacy in the House of Commons will not be a neutral interpretation, in fact such an interpretation is not possible, by anyone. The analysis will reflect my own cognition. While my knowledge,

values, and beliefs may be socially constructed, they are also my own, which means that the following work will reflect my own experiences and ideology.

Overview of this Chapter

The first section of this chapter, Politics and Power, will describe the defining characteristics of political discourse in the context of the debates that occur in the practice of Parliamentary democracy. This section will also will examine the role of power in political discourse, with a specific investigation of the ideological concept of 'common sense'.

While CDA is not a methodology unique to Fairclough, his version of CDA will guide and inform the analysis in Section 4.2. Using the method outlined in his book, *Language and Power,* 3rd ed., this section will describe the procedure and considerations of the first two stages of CDA through the analysis of a specific text from Hansard. The text and interpretation stages will analyze a debate on privacy that occurred on May 5, 2014.

Section 4.3 will conclude the chapter with the final stage of CDA, which is an examination of the text and the ways it which it shapes and represents the greater discursive and social practices within the House of Commons.

4.1 Politics and Power

The first purpose of this section will provide a further description of the characteristics of political discourse. This requires a general explanation of the idea of politics itself. The intent is not to provide a complete and conclusive definition of politics as a whole, but to single out the properties and characteristics of politics that will add to an understanding of how political texts are produced within the context of political activity. More specifically, this discussion will focus on the system of politics in Canada, as it was discussed in Chapter 1.

This discussion will provide the context for the second purpose, which is an examination of the ways in which power is distributed and maintained through political discourse, in this case, through the argumentative and deliberative aspects of political debate. This will include a discussion of ideology and 'common sense' within the context of political discourse.

What is Politics?

Politics, according to CDA scholar Teun van Dijk, can be described using a system of hierarchical categories ("Political Discourse Analysis" 16). As a preface to this description, it is important to note that Dijk's categorizations are simply meant to provide an insight into the relevant characteristics of politics in terms of understanding political discourse, and not as a prescriptive or singular treatment of the subject matter as a whole.

Politics itself exists as a broad societal domain, much like those of medicine, business, or education (Dijk, "Political Discourse Analysis" 16). Within the domain of politics are political systems, such as democracy, communism, or fascism, which serve to organize society in terms of the distribution of power, the style of economics, and the principles of decision making (Dijk, "Political Discourse Analysis" 16).

Political systems are informed by values and ideologies. Values are abstract convictions about what is important in a society, such as freedom, justice, or equality (Dijk, "Political Discourse Analysis" 16). Ideologies are informed by values, though they are harder to describe, as the meaning of ideology itself is a contested concept (Fairclough, *Language and Power* 35, 114). In terms of CDA, ideologies are representations of aspects of the real world that are built on systems of beliefs, values, and attitudes about the structure of society and how it should be sustained (Dijk, "Political Discourse Analysis" 17; Fairclough, *Language and Power* 32). Political systems, in many cases, are also political ideologies. To understand democracy as an actual structure that organizes and distributes power in society requires a deeper understanding of what democracy represents ideologically, such as the belief in the value of human rights, among other things.

Political institutions organize the field of politics and determine its function; these are things like city councils, Congress, or Parliament (Dijk, "Political Discourse Analysis" 17). This differs slightly from Fairclough's use of the word 'institution', the meaning in this context refers to the representation of the specific situational contexts where distinct types of political practice occurs, and not the specific location itself. Political institutions consist of political organizations that structure political action, such as political parties, which are also defined by

virtue of their distinct ideologies (Dijk, "Political Discourse Analysis" 17).

Less structured than political organizations are political groups, consisting of political actors. Groups of political actors may define themselves ideologically, for example, as demonstrators, strikers, lobbyists, dissidents, and so on (Dijk, "Political Discourse Analysis" 17). Political actors, as discussed earlier, can be all people who are engaged in politics, not just politicians who do the paid job of politics. More generally, political actors are those who participate in the political process by the act of voting (Dijk, "Political Discourse Analysis" 17). Independently, political actors are influenced by their own cognition and ideologies.

Connecting each of these political structures are political relations, which concern the ways in which social relationships are enacted, and ultimately, how power is distributed and maintained (Dijk, "Political Discourse Analysis" 17; Fairclough, *Language and Power* 13). Political relations are the interactions between the social structures, groups, and actors in the domain of politics and society as a whole, for example, how the government relates to its citizens or how political groups are positioned relative to others (Dijk, "Political Discourse Analysis" 17). Using Fairclough's terms, political relations are influenced by social orders and orders of political discourse that lead to the reproduction and occupation of political roles.

Political actions are concrete political events, carried out by political actors, and include the act of doing things like voting and passing laws (Dijk, "Political Discourse Analysis" 17). Political actions are based on the notion of political processes, which, much like social practices, represent the 'ways of doing' politics (Dijk, "Political Discourse Analysis" 18). Political discourse is the textual representation of political practice and interaction, through the production and interpretation of political texts, such as speeches and debates, propaganda, and advertising (Dijk, "Political Discourse Analysis" 18).

Using the preceding system of categorization as a guide, along with the general description of the organization of Canadian politics from Chapter 1, the context of the structure of the Canadian system of politics as it concerns the analysis in the next section is described in the following list:

- System: Democracy
- Institution: Parliament
- Values and Ideologies: Democracy, group and party ideologies
- Organizations: Political parties
- Political actors: Members of Parliament
- Political relations: Legislative power
- Political process: Legislation
- Political action: Political decision making, including legislating

What is Political Discourse?

The practice of 'doing politics', in the most general sense, involves making decisions about what to do and how to act in response to an event or a situation (Fairclough and Fairclough 58). Making decisions involves the process of deliberation, which requires a consideration of

potential courses of action that ultimately results in a normative judgment about what ought to be done (Fairclough and Fairclough 119, 765). Deliberation in politics is argumentative in nature; it is a discursive process where people give and receive reasons that attempt to justify or criticize a proposal for action that will result in a decision (Fairclough and Fairclough 102). Argumentation involves practical reasoning, which is the weighing of considerations for and against a particular action as a response to a practical, or 'real world' problem (Fairclough and Fairclough 69, 153). Practical reasoning in politics is characterized by uncertainty, as different political actors will interpret problems in different ways based on their own goals and cognition, as well as their own ideological perspective and that of their party (Fairclough and Fairclough 117-118). Political decisions are ultimately made in a context of disagreement, uncertainty, and risk, which is what makes deliberation with others essential in arriving at a reasonable decision, even though the decision may fall short of a normative ideal (Fairclough and Fairclough 104).

What is Parliamentary Discourse?

The political discourse under examination in this chapter occurs in the institutional context of Parliament, and more situationally within the House of Commons, where decisions are made through a procedurally regulated discursive practice known as debate. Using the above definition of political discourse, a political debate can be understood as a deliberative activity involving the process of practical argumentation that is oriented to a normative goal, with the added condition that the possibilities and outcomes are constrained by the institutional context of where the debate occurs.

These constraints affect the interactions that occur within the immediate situational context of the House of Commons. The House is subject to regulations involving when and how often sittings occur, with the minimum requirement that sittings happen once every twelve months (O'Brian and Bosc). Each sitting is regulated by a daily order of business, which is a schedule of events that determines when, and for how long political activities, such as debates, will take place (O'Brian and Bosc).

Debate, as a discursive political practice, is a highly regulated activity subject to a specific set of rules, which serve as further constraints. These rules include "limitations on what may be said, when and by whom it may be said, and for how long each debater may speak" (O'Brian and Bosc). Debates can only occur when there is a motion, which is a proposal made by an MP that asks the House to do something, order something done, or express an opinion on a matter (O'Brian and Bosc). Motions adhere to a specific style of wording, which uses affirmative, and not argumentative language (O'Brian and Bosc). The debate must follow a specific sequence of steps and the decision to adopt or defeat a motion is decided by means of a vote, where the majority of votes wins (O'Brian and Bosc).

Legislating is the most significant task in the House of Commons, and the process of debating and deciding on the standardized motions required for a Bill to become a law comprises the majority of the time spent by MPs in the House (O'Brian and Bosc). Due to the multi-party nature of the House of Commons, the resolution of disagreements through the process of practical argumentation does not necessarily mean that all of the participants

actually agree on what ought to be done (Fairclough and Fairclough 767). While the intent of the participants in the debate is to persuade others of their view, consensus is not necessary, only the mutual agreement that the results of the vote are binding (Fairclough and Fairclough 780). While MPs generally vote in accordance with the ideological views of their political party, this is not always a requirement; if this were the case there would be no reason for debates at all, as those in the majority would have the power to make the final decision on any motion (Fairclough and Fairclough 780).

It is important to recognize that the Canadian parliamentary system, at least in comparison to similar systems in Britain and Australia, upholds a very stringent practice of party discipline which is effectively controlled by each party's Whip (Library of Parliament, "Party Discipline" 1). The Whip is responsible for enforcing party discipline and ensuring attendance during Sittings, as well as other administrative and communicative tasks (O'Brian and Bosc). Party discipline means that the members of the same party vote the same way (Library of Parliament, "Party Discipline" 1). These 'whipped votes' are encouraged through the use of incentives, such as Cabinet or Parliamentary Secretary appointments, or punishment, which can include everything from less desirable assignments, to restrictions on travel, and removal from appointments or the even the party itself (Library of Parliament, "Party Discipline" 2). Though it is rare, 'free votes' do occasionally occur; these votes are usually concerned with questions of conscience or morality that transcend ideological party lines (Library of Parliament, "Party Discipline" 2). Free votes are a political matter, meaning there are no specific procedures in the House to regulate them (Library of Parliament, "Party Discipline" 2). When such a vote occurs, the free vote may be allowed by all parties, or by just one (Library of Parliament, "Party Discipline" 2).

As discussed in Chapter 1, the nature of a parliamentary democracy is one of imbalance, where one political party generally has more elected representation than the other parties. Party discipline is especially significant during periods of minority governance, where the outcome of votes can be seriously affected by the number of MPs in attendance. Though there are periods of minority governance in the Hansard corpus, the period under examination in this chapter had a majority government. Out of 308 available seats in the House, the government held 160 seats as of April 10, 2014, leaving the remaining 148 seats for the other members of the opposition parties, 99 of which were filled by the Official Opposition (Library of Parliament, "Parliaments").

The function of parliamentary debate is also highly performative, as the proceedings of the Sittings in the House of Commons are televised, in what has been called 'gavel-to-gavel' coverage (Robertson 1). The recording of the proceedings is subject to guidelines, which include the use of specific camera angles and restrictions on microphone range (O'Brian and Bosc). During debate, MPs occasionally speak to the 'folks back home', or refer to the 'people listening' or 'turning on their TV' (*Hansard Vol. 147 No. 80,* 4903, 4909, 4938). This combination of TV coverage, the print and digital Hansard, the resulting media coverage, and the political memory of both the MPs and the public combine to create what Fairclough calls "intertextual context" (*Language and Power* 164).

Intertextual context relates to the 'history' of texts within a discourse, in that they have a

historical relationship to the series of texts that have come before them (Fairclough, *Language and Power* 164). This historical relationship allows both the producers and the interpreters of the discourse to make presuppositions about content and context based on their prior knowledge of the discourse (Fairclough, *Language and Power* 164). But presuppositions are essentially assumptions, and in the case of the text producer, these assumptions presuppose an ideal reader or audience that may not actually exist (Fairclough, *Language and Power* 165). In the case of the actual interpretation of the text, presuppositions may draw on the cognition of the text consumer in a way that is accurate, or in a way that is not, which means that there is power in the ability to determine the intertextual context of a discourse ((Fairclough, *Language and Power* 165).

Language and Power

In this way, presuppositions can be seen to be ideological because what is assumed by a text producer may or may not be understood by the interpreter of the text, and since presuppositions refer to an implied history of the text, rather than an explicit description, they may be difficult to recognize, and if they are misleading or false, refute (Fairclough, *Language and Power* 165). Intertextual context in parliamentary debate is a discursive constraint; the power is in the ability of the text producers (the MPs) to manipulate the interpretation of the text (the debate) through references to the background information and cognition of the intended audience (the public and other MPs) through implicit references to experiences which the producer may want the audience to accept as historically or factually accurate (Fairclough, *Language and Power* 165). These presuppositions, whether sincere or manipulative, are inevitably reproduced by other MPs, the media, and the public, which can have the effect of imposing an ideological proposition into the social cognition of those without enough knowledge of the historical context of the discourse to challenge it (Fairclough, *Language and Power* 165).

Another ideological dimension that influences the intertextual contexts in parliamentary debates are the competing and contradictory presuppositions that may be referenced by MPs from different political parties. Party discipline ensures that MPs are consistent in the ways in which they vote on motions, and this discipline extends into the discourse in the shared construction of history within and across the parties themselves. Presuppositions allow MPs to draw on complex orders of discourse in the short amount of time they are afforded to speak to an issue in the House. In many ways, these presuppositions contribute to the adversarial nature of the 'political theatre' that results from the performative nature of televised debates (Harris 467). The primary role of opposition MPs is to oppose the policies and positions of the government as a whole; this is accomplished through the use of language that undermines the credibility and competence of their adversaries, the government MPs (Harris 466). The governing party can control the debate by constantly shifting the agenda in favour of discussing their own positive achievements, thereby undermining the criticism of the opposition (Harris 467). Televised debates enhance this confrontational process by allowing MPs from opposite sides of the House to be 'seen' as adversaries, stepping up to face each other while playing their distinct and recognizable roles (Harris 467).

Intertextual presuppositions are a multifaceted example of discursive constraints, because the struggle for power in the discourse occurs across multiple modes. Discourse constraints, in

general, can be separated into three broad but overlapping categories: content, which is what can be said or done; relations, which involve social relations within discourse; and subject, which are the 'subject positions' people can occupy (Fairclough, *Language and Power* 76). These constraints affect the immediate situational context of discourse, but they also exert a broader structural influence across orders of discourse (Fairclough, *Language and Power* 98).

Political debates have many other content constraints. In addition to those already discussed, debates in the House must focus on one motion at a time and no other motions may be discussed until the matter has concluded in some way (O'Brian and Bosc). Relational constraints concern the relationships among the discourse participants; for example, party discipline dictates that the members of each party are in a subordinate relationship to their Whip, as well as their party's leader (O'Brian and Bosc). Subject position refers to the roles available to the discourse participants, for example, one of the subject constraints in the House concerns the role of the Speaker, who must be elected by the Members of the House itself; other MPs cannot just step in and assume the role (O'Brian and Bosc). Content, relational, and subject position constraints overlap in terms of the imbalance of power inherent within the House itself. The government, by nature of the number of elected MPs, gets to talk more, sets more of the agenda, has a stronger influence on the outcome of votes, and retains executive powers for implementing government policies and programs (O'Brian and Bosc).The process of parliamentary debate, especially during a majority, serves to legitimize the power of the governing party through a public display of their openness to the consideration of opposing viewpoints, despite the reality that the distribution of votes will always support the ideological aims of the government.

Fairclough describes this as 'power in discourse', where powerful participants "control and constrain the contributions of non-powerful participants" (*Language and Power* 75-76). Power in discourse is the expression of power within the discourse itself, and it can be determined through an examination of the constraints faced by the discourse participants in terms of their social roles and the effect they have on relations and content.

'Power behind discourse' refers to orders of discourse and how they are communicated and maintained through the hidden effect of power (Fairclough, *Language and Power* 83). In terms of parliamentary debate, the constraints created by the power behind discourse have to do with access (Fairclough, *Language and Power* 89). Discourse involves the production and interpretation of texts, and in this case the text is Hansard. While Hansard is primarily associated with MPs, they are not the only political actors. Yet, as it was discussed in the previous section, only MPs may participate in the debates, which happens as a result of their access to the knowledge and beliefs, social relationships, and social roles associated with 'doing politics' (Fairclough, *Language and Power* 99).

Access to politics uncovers a number of interrelated issues in terms of the power behind discourse. In order to become an MP, a person must first be elected. In order to get elected, or to even try to get elected, that person needs to have access to the development of the skills and knowledge that underlie the social role of politician; something that requires financial resources and the support of a local riding association. This requires having early access to

literacy (Fairclough, *Language and Power* 90), which determines access to a certain quality of childhood education, which determines access to post-secondary education, which determines access to skilled professions, which determines access to the finances and social relationships required to participate in a political election. Having access to the skills and knowledge required to fulfill the social role of politician doesn't guarantee that one will get elected, nor does it mean that someone with less access won't find success in politics, but access is a constraint based in power nonetheless.

The power behind this discourse is apparent in the reproduction. When a social role is consistently reproduced with little variation, the discourse associated with the representation of that role becomes prioritized to the point of seeming natural (Fairclough, *Language and Power* 113). In the case of becoming a politician, it seems completely natural that the role should require special skills and knowledge. This is reinforced in one way by the formality inherent to the discourse of parliamentary debate. People that lack access to the specialized training and literacy skills that are required to engage in debate may see the formality of the language as a barrier to participating. Fairclough describes this as a constraint on language form, which in turn creates an imbalance of power between those with access and those without (Fairclough, *Language and Power* 93). This constraint not only restricts access to the social role, but it generates an aura of awe around the role itself (Fairclough, *Language and Power* 114). This awe serves to further naturalize the exclusivity of the social role of politician.

Naturalization occurs when one type of discourse becomes so dominant within a domain or institution that it seems as though there couldn't possibly exist any other alternatives (Fairclough, *Language and Power* 113). While the discursive practice of debate contributes to the power inherent to the social role of politician, it also exerts an influence on relational and structural imbalances. Political debates literally control the legislative power within the House of Commons, as political decisions are not made unless a motion, debate, and vote occurs. The decisions that are made affect all political actors, not just politicians. But debate is not the only way to make a decision as a group; an alternative discourse type for parliamentary democracies could involve a model of consensus-based decision making. The fact that parliamentary democracies rely exclusively on debate for decision making appears to be 'common sense' because the discourse type has been so naturalized within the institution that it seems like the only legitimate way to proceed.

Naturalization and common sense are grounded ideologically (Fairclough, *Language and Power* 113). Debate as a discourse type is valued over other types of discourse in parliaments because of the power it affords to those who control the institution, as the nature of majority decision making keeps power in the hands of the majority. Though the majority in a parliament may change as a result of elections (which in itself is an ideological issue), the dominance of the discourse type doesn't. The result of this naturalization is that the discourse type becomes so enmeshed in the structure of the institution that its ideological character becomes hard to distinguish (Fairclough, *Language and Power* 113).

The influence of common sense can also affect the meaning of individual words (Fairclough, *Language and Power* 115). What Fairclough describes as the 'meaning systems' of words was

introduced in the last chapter as collocation. This is the idea that individual words can "acquire implications" when they occur repeatedly with other words (Stubbs, "Words and Phrases" 7). When language users understand meaning systems implicitly, it becomes a matter of common sense that certain words will have a fixed definition when they occur with other words (Fairclough, *Language and Power* 115). Meaning systems are especially problematic in terms of discourse prosody, which is the idea that when a word frequently occurs in a context that is clearly positive or negative, uses of the word in other contexts may carry the same implied attitudinal meaning (Hunston, "Semantic Prosody Revisited" 250).

When meaning systems become common sense, they appear to lose their ideological character, which creates an impression that certain words and phrases can only be interpreted one way (Fairclough, *Language and Power* 116). This has the effect of constraining the content within the discourse because controlling the meaning of the language controls the discourse itself, especially when words with seemingly fixed definitions are used to manipulate those with less power in the interaction. When fixed definitions of words travel across discourse types, they have the power to maintain whole orders of discourse through the fixed determination of accepted knowledge and beliefs about certain topics, relationships, and social roles (Fairclough, *Language and Power* 99, 116).

Power is maintained through the reproduction of orders of discourse when there is little to no variation. When meaning systems, perceptions about social roles and relationships, and the structural nature of institutions become internalized in cognition, they become common sense. The more people that internalize the common sense ideas, the more they are reproduced, and the harder they are to change. This is how power is maintained through hegemony. There is no need to coerce people into giving up their power when they believe that imbalance in society is just common sense.

The next section will describe the method of conducting CDA by examining a specific selection of discourse from Hansard. The CDA will integrate the results of the text analysis in Chapter 3, the discussion on privacy from Chapter 2, as well as many of the topics discussed in this section. The method of CDA, as it was described earlier, involves three interrelated areas of analysis: text, interpretation, and context. The text analysis conducted in the last chapter identified specific trends from Hansard that were deemed worthy of examination, some of which will be further explored by the CDA. Chapter 2 introduced the concept of privacy and the legislation and jurisprudence of privacy in Canada, which will serve to focus the analysis. This section contained elements of the interactional and contextual analysis, describing the immediate interactional context of the House of Commons in which the discourse appears, as well as the broader orders of discourse that the House draws upon. The first two stages of the CDA will be interwoven in the next section, the results of which will be discussed as the third stage of analysis in the concluding section of this chapter.

4.2 Text and Interpretation

The analysis in this section will both describe and carry out the method of CDA using a transcript from the Hansard corpus. The method of CDA comes directly from Fairclough's *Language and Power*, 3rd ed., which outlines his theory and process. While Fairclough's method is not the only approach to CDA, it will form the basis of the analysis that follows here.

Fairclough's method is based on a three part analysis of text, interpretation, and context. The first stage involves the investigation of a text in terms of the formal properties of language: the actual words, phrases, and sentences, in terms of vocabulary, grammar, and overall structure (*Language and Power* 129). The second stage is an interpretation of the social content of the discourse, which includes interpreting the interactions between the discourse participants and each other and within the situational context where the discourse occurs, as well the interactional nature of the discourse itself (Fairclough, *Language and Power* 154). The third stage is an explanation of the relationship between the discourse and the social structures it represents in an attempt to contextualize the discourse as a social practice that sustains or changes relations of power in society (Fairclough, *Language and Power* 172).

The goal of this entire work has been to investigate the discourse of privacy in the House of Commons in an attempt to determine the meaning of the word as it is used in practice. An analysis of this nature does not lend itself to linearity, in fact it has been continuously undertaken throughout every chapter so far. Chapter 1, the Introduction, described the basic structure of the Canadian federal system of government. This description fits into stage two of CDA, as it provided information about the situational context of the House of Commons, where the discourse occurred.

Chapter 2 was an investigation of federal privacy legislation and the ways that the legislation has been interpreted by the Supreme Court. It also included an examination of documents and philosophy that influenced the both the creation of the privacy legislation and the rulings of individual court cases on privacy issues. This provided further information for stages one, two, and three. The description of the content of the actual legislation and the court rulings fits into stage one. The legislation itself is created in part through the discursive practice of debate. While the House of Commons is responsible for the production of the legislation, it is interpreted by the courts, with the Supreme Court acting as the final and ultimate arbitrator. The resulting court judgments and the legislation itself is further interpreted through debate in the House. This examination of the relationship between the legislation and the Supreme Court rulings, as well as the context under which both were created fits into stage two. The power in the House of Commons is expressed and sustained through the enactment of legislation, which in most cases is based on the ideology of the majority government. This legislative power can either be maintained or challenged by the courts. Both of these factors provides the context for stage three.

Chapter 3 involved a text analysis of the Hansard corpus spanning the whole of the 39th to 41st Parliaments. This time frame represents the entire period of minority and majority governance by the Conservative Party of Canada under the Right Honourable Stephen Harper.

The text analysis investigated the formal language use during this period by determining the frequency of the word 'privacy,' as well as the frequency of phrases related to privacy, those being 'privacy rights', 'right to privacy', and 'reasonable expectation of privacy'. Concordance and collocational analyses were also conducted, which uncovered trends related to the 'meaning systems' that encompass the word privacy. These trends include a verification through collocational statistics that the word 'right' is strongly associated with 'privacy in a non-random way. The concordances revealed trends regarding the use of 'privacy' at the level of the sentence, which identified a clear relationship between 'privacy' and social groups, the most interesting of these was a group repeatedly identified as 'law-abiding' Canadians. Chapter 3 clearly fits into stage one of the CDA method. Furthermore, while this section is focused on the formal analysis of one specific instance of discourse, the results of the text analysis in Chapter 3 help to situate the discourse within the broader context of social interactions and structure in the House as a whole, which helps to validate the interpretation and explanation required for stages two and three

Finally, this chapter provided further insight into the specific discursive practice of debate and the ways in which it contributes to the structure of the House of Commons. The previous section in this chapter described the relationships between the Members of the House and each other, as well as their relationship to the House itself, which fits into stage two. The struggle for power enacted through these interactions and the situation context as a whole were described in terms of the constraints that mediate the social and structural relationships, which fits into stage three of the analysis.

The specific transcript for the CDA was selected based on the results of the text analysis in the Chapter 3, which showed trends related to an increase in the relative frequency of the word privacy in 2014, as well as increase related to the phrase 'privacy rights'. Out of a total raw frequency of 1567 occurrences of 'privacy' in 2014, the transcript for May 5, 2014 contained the highest raw and relative frequencies of any of the transcripts that year, totaling 243 instances of the word, for a relative frequency of 0.43% compared to the total words in the transcript. The phrase 'privacy rights' occurred 101 times in 2014, and 16 of those times occurred on May 5, 2014, which was again the highest raw frequency for that phrase in 2014. The relative frequency of the phrase compared to the total number of words was 0.028%. This data is articulated in Table 4-6.

	privacy		privacy rights	
Period	2014	May 5	2014	May 5
Raw Frequency	1567	243	101	16
Ratio %	0.022	0.43	0.0014	0.028

Table 4-6: Comparison of raw and relative frequencies of 'privacy and 'privacy rights'

As it was just mentioned, CDA is not a linear process. To serve the purpose in this chapter of describing method and analysis concurrently, Fairclough's three stages of CDA will be presented as separate parts. Though in order to understand the content of the formal analysis of the text itself, the context of the interaction must first be described as a means of 'setting the stage' for the entire analysis. Though much of this work has already been done, the analysis will begin with stage two, the interpretation of the discourse interaction, and

then move back to stage one, the textual properties of the discourse itself. Stage three, the explanation stage will be presented in the next section, as a means of concluding the chapter.

Stage Two: Interpretation

The purpose of the interpretation stage is to determine the ways in which the relations between the discourse participants and the situational context of the discourse play a role in the production and interpretation of the discourse itself. Fairclough has structured the interpretation stage with a number of guiding questions that have the purpose of determining the content, relations, and context of the discourse beyond the level of individual words and sentences (*Language and Power* 159). While the discourse type and situational context have already been described, the following text will provide further details about the content of the discourse itself and the social roles and relations of the discourse participants.

What's Going On?

As a way of balancing the competing interests of the opposition parties in the House, there are 22 'alloted days' in a calendar year specified for the business of supply (Parliament of Canada, "Business of Supply"). On supply days, as they are commonly called, opposition motions take precedence over all government business (Parliament of Canada, "Business of Supply"). Opposition motions can be proposed by any of the opposition parties, and not just the Official Opposition, though the opposition parties must decide amongst themselves who will sponsor the motion ("Opposition Motions"). The transcript selected for this analysis occurred on one such supply day.

The text concerns a motion proposed by the Official Opposition. The motion led to a debate which lasted several hours and included a number of participants from four different political parties.

The motion was proposed by Charmaine Borg, an NDP MP representing the Quebec riding of Terrebonne—Blainville. At the time, Borg was the Digital Issues Critic and a member of the Standing Committee on Ethics, Privacy and Access to Information. The motion is as follows:

> That, in the opinion of the House, the government should follow the advice of the Privacy Commissioner and make public the number of warrantless disclosures made by telecommunications companies at the request of federal departments and agencies; and immediately close the loophole that has allowed the indiscriminate disclosure of the personal information of law-abiding Canadians without a warrant (*Hansard Vol. 147 No. 80,* 4899).

In this motion, Borg is advancing two proposals. The first proposal is that the government should follow the advice of the Privacy Commissioner by publicly disclosing the number of times that personal information about Canadians was provided to federal departments and agencies without a warrant.

The second proposal suggests that the government "close the loophole" that allows federal departments and agencies to obtain access to personal information about "law-abiding

Canadians" without first applying for a warrant.

In the speech accompanying the motion, Borg explains that she has proposed the motion in response to a recent revelation from the Privacy Commissioner Chantal Bernier. Bernier announced that during 2011 federal agencies made 1.2 million requests to telecommunications companies for the personal information of subscribers without first obtaining a warrant (Hennessey). This information is contained in a letter dated December 14, 2011, addressed to former Privacy Commissioner Jennifer Stoddart from Karen E. Hennessey of the law firm Gowling LaFleur Henderson. The letter is a response to a request from Stoddart for information regarding the number and nature of requests for personal information made to telecommunications companies by federal and law enforcement agencies. This letter can be found in Appendix 1.

Stoddart's letter also requested information about whether the telecom companies publicly disclosed the number of requests, if they notified customers to give them an opportunity to appeal the disclosure, whether fees are requested, and if deep-packet inspection is used (Hennessey). Interestingly, the request was mediated through a law firm to provide for the anonymity of the nine agencies that responded. This is despite the fact that none of the companies notified the subscribers about the disclosure of their personal information.

This debate occurred before Bill C-13, otherwise known as the Protecting Canadians from Online Crime Act, came into force. As it was discussed in Chapter 2, Bill C-13 contains an addition that allows peace or public officers to request the voluntary disclosure of data if there is no legal reason why it cannot be disclosed. Though the bill had not yet come into force, the Members of the House were aware of it, and based on the content of many of the speeches in this debate, the bill was seen by the opposition parties as further eroding the privacy protections afforded to Canadians under the legislation at the time. So although the motion was technically about the state of the legislation on May 5, 2014, it became a way for the Official Opposition to raise their objections in anticipation of Bill C-13.

For the government, the debate on the motion was a way for them to further justify their reasons for supporting Bill C-13, as well as to voice their support for Bill S-4, The Digital Privacy Act, which as discussed in Chapter 2, contained amendments to PIPEDA. These amendments had also yet to come into force.

Who's Involved?

Appendix 2 contains a complete breakdown of the individual speakers by party, including the number of times they spoke, as well as the ratio of their contribution to the total number of speeches in the debate. The way in which Hansard is formatted in print makes it easy to determine who has spoken, what they have said, and when they have said it within five minute intervals. The number of instances of individual speech was determined by extracting all of the names from the text of the debate itself and counting them, regardless of repetition. The number of speakers was determined by counting the total number of unique names in the list. While other business was discussed in the House that day, the analysis here is focused only on the text directly involved in the debate, meaning the count of speakers and speeches in the

transcript as a whole is different than the count of speakers and speeches within the context of the debate itself.

What are the Relations?

The House of Commons is based on the idea of representation. MPs are elected to represent the people in their electoral district, which consist of specific areas demarcated by geography. The number of seats in the House is decided on the basis of population figures, which divide the country into a total of 308 electoral districts based on province or territory (O'Brian and Bosc). In theory, when MPs speak in the House, they are speaking on behalf of all of those who reside in a particular area of geography.

Another aspect of representation has to do with political party membership. While MPs are representative of their electoral district, they also represent the ideology of the political party they belong to. At the time of the selected transcript there were five different political parties represented by MPs in the House of Commons. While this analysis is a non-partisan investigation of the discourse of privacy as it is represented by the House of Commons as a whole, it has to be recognized that there are competing orders of discourse within the House itself, based on differences in party ideology.

The nature of party discipline requires MPs to effectively balance these two distinct relationships (Library of Parliament, "Party Discipline" 2). While MPs are responsible for voicing the concerns and wishes of their constituency, they must also consistently maintain a viewpoint that aligns with their chosen party's ideology (Library of Parliament, "Party Discipline" 2).

Table 4-7 shows the breakdown of speakers and speeches by party, as well as the total distribution of seats by party in the house (Library of Parliament, "Parliaments"). The Official Opposition, the New Democratic Party (NDP), had the highest number of speakers and speeches, at 48% and 46% respectively. The government, the Conservative Party (CPC), came in at second place with a 36% of the total speakers and 36% of the speeches. The other

Party	Total Seats		Speakers in Debate			Speeches in Debate	
	number	% total seats	number	% total seats	% within debate	number	% within debate
Conservative Party	160	51.9%	11	3.6%	35.5%	38	35.8%
New Democratic Party	99	32.1%	15	4.9%	48.4%	49	46.2%
Liberal Party	35	11.4%	4	1.3%	12.9%	18	17.0%
Bloc Quebecois Party	4	1.3%					
Independent	3	1.0%					
Green Party	2	0.6%	1	0.3%	3.2%	1	0.9%
Vacant	5	1.6%					
Total	308	100.0%	31	10.1%	100.0%	106	100.0%

Table 4-7: Distribution of seats in the House by party compared to number of speakers and speeches in the debate

opposition parties, the Liberal Party and the Green Party, occupied the third and fourth place in this regard. During a debate, the Speaker of the House chooses who will speak based on a number of criteria (O'Brian and Bosc). On supply days, Members from the party sponsoring the motion may be recognized more frequently, which appears to be what happened in this debate (O'Brian and Bosc). Another reason for the reduced participation by the Members from the CPC may be their attitudes regarding the importance of supply days. This is illustrated by an excerpt from a CPC MP in the next section, where the MP explains that supply days are usually a waste of his time.

What is the Role of Language in What's Going On?

While a comprehensive text analysis was conducted in Chapter 3, the purpose of this further analysis is to investigate the actual instances of text in the context of the discourse to develop a deeper understanding of the language in use.

While it must be acknowledged that a single text can only represent a distinct moment in time, this text is the most substantive debate on privacy in all of 2014, which was a year where privacy was discussed with a greater relative frequency than the other years in the corpus. According to Sullivan, "when the purpose of a provision is discussed or its meaning explained during the enactment process, and the legislation is then passed on that understanding, the explanation or discussion offers persuasive (if not conclusive) evidence of the legislature's intent" (659). Therefore, this text can be seen to be representative of the cognition and ideology of the discourse participants, which provides evidence for their deeper understanding of the issue of privacy as a whole, and their motivations for supporting or opposing the legislation they are discussing. The debate selected for this analysis was, for all intents and purposes, a debate on Bill C-13, which made critical amendments to the Criminal Code in terms of an individual's reasonable expectation of privacy, which has a direct effect on individuals rights under s. 8 of the Charter to be free from unreasonable search and seizure.

Thus, the systems of meaning identified through the language used in this debate are representative of the orders of discourse that inform the true intent of the ideological understanding of privacy in the House of Commons.

Stage One: Text

Text analysis in CDA involves analyzing a text in terms of its vocabulary, grammar, and structure. The purpose of this level of analysis is to evaluate the text as a means of determining the systems of meaning and discourse type that the text draws upon, which can then reveal the ideological character of the language (Fairclough, *Language and Power* 128). The intent of this stage is not to examine all of the textual elements of the debate in its entirety, but to focus in on the specific elements that support the work that has already occurred.

Since a comprehensive text analysis has already been conducted on the corpus as a whole, this analysis will focus on three themes that have arisen as a result of that analysis, as well as from the privacy review in Chapter 2. These themes include the following: the right to privacy, the definition of personal information, and law-abiding Canadians.

The Right to Privacy

The text analysis in Chapter 3 uncovered a strong collocational relationship between the words 'privacy' and 'right'. This particular debate also had the highest frequency of the phrase 'privacy rights' compared to any of the transcripts in 2014. This phrase occurred most often in sentences that also included a reference to 'Canadians' or 'law-abiding Canadians'. The concept of 'law-abiding Canadians' will be investigated at the end of this section, but the concept of privacy as a right merits further discussion here.

The investigation in Chapter 2 concluded that Canadians do not have an explicit 'right to privacy', but rather, a quasi-constitutional right to the protection of their personal information held by government or business where a reasonable expectation of privacy exists. *R. v. Spencer* used s. 8 of the Charter as a privacy defence, specifically against warrantless search and seizure involving the disclosure of personal information, but when this debate occurred the judgment had yet to be published. The uncertainty surrounding the interpretation of the legislation responsible for protecting personal information, especially regarding the need to obtain a warrant, is evident in this debate.

During the course of the debate, four different CPC MPs conflate the rights afforded by the Charter and the legislation responsible for the protection of personal information as being one and the same, in a sense, referring to a Charter right to privacy. They all spoke with certainty that the Charter was directly responsible for the protection of personal information.

Dave Van Kesteren of the CPC made the most explicit statement, going so far as to say that privacy is guaranteed by the Charter:

> At all times an individual's right to privacy, as guaranteed by the Canadian Charter of Rights and Freedoms, must be respected. Despite any exception provided for in PIPEDA, law enforcement agencies must respect the charter and have a warrant or other justification to obtain private information (*Hansard Vol. 147 No. 80,* 4906).

Later, Paul Calandra of the CPC said that "(p)ersonal information that is protected by the charter requires a warrant" (*Hansard Vol. 147 No. 80,* 4922).

David Wilks of the CPC made the following remark:

> To be quite clear on this, an individual's private information that is protected under the charter cannot be released without a warrant. Police officers and other enforcement agencies in Canada are well aware of that fact (*Hansard Vol. 147 No. 80,* 4943)

In the next excerpt, Don Davies of the NDP was expanding on a comment made by his NDP colleague, Linda Duncan. Duncan and Davies, both former lawyers, were questioning Wilks, a former policeman, about an assertion he made that there is "no such thing as a warrantless search" (*Hansard Vol. 147 No. 80,* 4945). The exchange was antagonistic. Wilks asked Davies to provide a definition of warrantless search, and Davies' responded by saying that "it is fortunate to have a police officer asking a lawyer about the law" (*Hansard Vol. 147 No. 80,*

4945), leading Wilks to give the response, "I never listen to lawyers" (*Hansard Vol. 147 No. 80,* 4945). Duncan followed up with a comment implying that seeing evidence in "plain view" could be considered "reasonable cause" for a warrantless search (*Hansard Vol. 147 No. 80,* 4945). The exchange ended with Davies saying that "it would seem that nobody on that side of the House is aware of the Charter of Rights and Freedoms or how the Constitution works in this country" (*Hansard Vol. 147 No. 80,* 4946).

By 'that side of the house', Davies is referring to the seats occupied by the government, as the House is arranged in such a way that government MPs sit on one side, and opposition MPs on the other. Davies' statement had the likely intent of further antagonizing Wilks and the government as a whole, rather than pointing out that the Charter is not responsible for the protection of personal information, but this is as close as any of the MPs come to refuting the claims of the CPC.

Finally, Colin Carrie of the CPC made this remark: "Let me be clear. An individual's private information is protected under the charter and cannot be released without a warrant" (*Hansard Vol. 147 No. 80,* 4949).

What's interesting about these statements is their similarity. With the exception of the first comment made by Van Kesteren and the rebuttal by Davies, each person says something to the effect of 'personal information that is protected by the Charter cannot be released without a warrant'. Two of the four MPs prefaced the remark with a statement about 'being 'clear', which is a phrase that suggests transparency, but is also authoritative. The phrase is meaningless in these two contexts because what it is supporting has no basis in truth. The Charter, specifically s. 8, only affords individuals the freedom from unreasonable search and seizure. It does not purport to protect anything, certainly not personal information.

Considering the purpose of the motion, which was to discuss the 1.2 million warrantless requests by federal agencies for personal information, the identical statements by the CPC MPs have the appearance of being highly scripted, which is a clear indication of the far-reaching influence of party discipline. What kind of personal information are the CPC MPs referring to when they speak of the protection afforded by the Charter?

Basic Subscriber Information

The definition of personal information was discussed at length in this debate, though it was referred to primarily as 'basic subscriber information'. In all, this term appeared 41 times.

Basic subscriber information, according to Members of the CPC, consists of a individual's name, phone number, address, email, and IP address (*Hansard Vol. 147 No. 80,* 4908, 4915, 4940, 4950). Part of this definition appears to come from Bell Canada, as a statement from a Bell spokesperson is quoted or referenced by CPC Members five times during the debate (*Hansard Vol. 147 No. 80,* 4905, 4932, 4941, 4949). The statement was first shared in full by Roxanne James, and then by Blake Richards:

Bell will only provide law enforcement and other authorized agencies with basic 411-style

> customer information such as name and address, which is defined as non-confidential and regulated by the CRTC [...] Any further information, or anything related to an unlisted number, requires a court order. (*Hansard Vol. 147 No. 80,* 4932, 4941)

This statement does not include a reference to an email address or IP address, so it is unclear what the basis for the CPC definition truly is. Neither the Privacy Act, nor PIPEDA provide a specific definition of personal information. PIPEDA describes personal information as "information about an identifiable individual", and the definition in the Privacy Act is identical to PIPEDA, except that it includes "that is recorded in any form" at the end.

This phone book or '411' analogy was used repeatedly by CPC MPs, seemingly as a way to normalize the disclosure of basic subscriber information as a routine practice of law enforcement required to prevent serious crimes (*Hansard Vol. 147 No. 80,* 4904, 4907, 4932, 4933, 4940, 4941, 4943, 4945, 4950, 4951). CPC MPs also repeatedly pointed out that the information was provided on a voluntary basis by telecommunications companies (*Hansard Vol. 147 No. 80,* 4904, 4907, 4933, 4934, 4935). What's interesting about this analogy is that if the information was as readily available as information in phone book, the police wouldn't need to make a request for it, because they could just look it up themselves, as could anyone.

Adding the statement about voluntary disclosure shifts the responsibility away from the police and on to the telecommunications companies who provide the information. Roxanne James of the CPC, wants to be "perfectly clear" with the following statement:

> We expect that telecommunication service providers abide both by the law and their agreements with their customers in terms of what they release to law enforcement and when they do so. (...)
> We expect that telecommunication service providers only release basic subscriber information when it is for reasons of public good, such as to help police investigating a crime or, for example, identifying the next of kin (*Hansard Vol. 147 No. 80,* 4932).

Carrie, in a continuation of his earlier "let me be clear" statement about the protection of personal information by the Charter made this remark:

> The telecommunications companies have already said that they only release 411 style information. In other words, like in the old days when we were younger, there was a reverse lookup for a telephone number. This is the type of information that is being disclosed, and we fully expect these companies to comply with the law and play by the rules when handling the private information of Canadians. (*Hansard Vol. 147 No. 80,* 4949)

Comparing the disclosure of basic subscriber information to what is available through 411, and referencing the 'old days' of reverse lookup for telephones, is creating an analogous relationship between two distinctly different types of information: an IP address and a phone number. Fairclough argues that metaphors and analogies are ideological in that they tend to frame the interests that are dominant in the discourse as interests that are important

to society as a whole, while construing non-dominant interests as undermining or harming society in some way (*Language and Power* 137).

The CPC use of the phone book analogy fits into this description. Their argument for the 'voluntary' disclosure of basic subscriber information is based on the need for law enforcement to have immediate access to information that may prevent or stop serious crimes, and also as a way of protecting "young people, children, and seniors" (Kesteren, *Hansard Vol. 147 No. 80,* 4907). Their description of the crimes that this immediate access to basic subscriber information will prevent is far-reaching. Hon. Michelle Rempel of the CPC made this remark:

> It is used by authorities for things like investigating Internet fraud or other online crimes, notifying next of kin after a traffic accident, addressing suicide threats over crisis lines, returning stolen property to rightful owners, or investigating threats posted on or sent over the Internet. (*Hansard Vol. 147 No. 80,* 4915).

While Blake Richards made the following statement:

> These activities run the full gambit, whether they are trying to bust a drug gang or human smuggling ring, investigating a threat of physical violence, or trying to identify anonymous child predators who are distributing child abuse images on the Internet (...) Police need access to basic subscriber information to do this critical work, to keep Canadians safe from these criminal activities. In some cases, this is the only avenue to advance a criminal investigation. (*Hansard Vol. 147 No. 80,* 4940)

By linking the urgent need for 'voluntary' disclosure with the prevention of crimes, especially crimes against young people, children, and seniors, the CPC are using the phone book analogy to imply that it would be harmful to society if information was not readily available. The way they've framed their argument makes disagreement akin to supporting crime. This is not a new strategy for the CPC, and three NDP MPs picked up on this implication.

Through the course of the debate, NDP MPs Charlie Angus, Ryan Cleary, and Dany Morin each made a reference to something that had happened in the House two years earlier. This was the Protecting Children from Internet Predators Act, or Bill C-30, which was discussed on February 13, 2012 (*Hansard Vol. 146 No. 79,* 5196) before being introduced the next day by the former CPC Minister of Public Safety, Vic Toews (LEGISInfo). The Bill, also known as the Lawful Access Act, was incredibly controversial, not just because of what it proposed, but because of Toews himself (Austin 111). In his justification for the Bill, Toews famously said to an opposition MP from the Liberal Party that the MP could "either stand with us or with the child pornographers" (*Hansard Vol. 146 No. 79,* 5196). Bill C-30 was withdrawn before it could reach a second reading (LEGISInfo).

Critics and MPs have argued that Bill C-30 and Bill C-13 (which is the implicit focus of this debate) are in many ways the same. The key difference between them is the wording; where Bill C-30 allowed for 'mandatory warrantless access', this has been rephrased in Bill C-13 as 'lawful access' (Austin 111-112). The result, according to Austin, was that the intent of Bill

C-13 required interpretation by the courts, which ultimately culminated in the ruling of *R. v. Spencer* (Austin 113).

By bringing up the past, the NDP MPs drew upon the intertextual context of the House of Commons with a presupposition that implied that the current motion under debate was just as controversial as the incident two years earlier with Toews. Angus described the issue of warrantless requests for personal information as the "revenge of Vic Toews" (*Hansard Vol. 147 No. 80,* 4902). Cleary called the dead Bill C-30 "outrageous" and reminded the House of the backlash by saying that "Toews was appointed to the Manitoba bench" as a result (*Hansard Vol. 147 No. 80,* 4914). Morin described both Bill C-30 and Bill-13 as being "basically the same", and called out the comment by Toews as an "utterly reprehensible thing to say" (*Hansard Vol. 147 No. 80,* 4938).

Returning now to the phone book analogy, opposition MPs questioned whether an IP address was really an example of 411-style information. NDP MP Angus quoted Ontario Privacy Commissioner Ann Cavoukian when she said:

> ...customer name and address information ties us to our entire digital life, unlike a stationary street address. Therefore, "subscriber information" is far from the modern day equivalent of a publicly available "phone book". Rather, it is the key to a much wider subset of information. (*Hansard Vol. 147 No. 80,* 4902)

This statement precisely articulates the difference between personal information about identity (such as a name or a phone number) and personal information that serves the purpose of identification, a concept that was discussed in Chapter 2. While a name, phone number, and address is personal information about identity, an IP address serves the purpose of identification by adding value to the information about identity. Borg, the MP who proposed the motion for this debate, describes this distinction in terms of Wi-Fi use, saying that "in some cases, (an IP address) could tell where someone has been, (and) what they are doing" (*Hansard Vol. 147 No. 80,* 4941).

The concern about IP addresses created another antagonistic exchange, this time between CPC MP Mike Wallace and Liberal MP Scott Andrews. Wallace begins a lengthy statement by expressing that "in the past some of the topics that have been brought forward on supply days (...) were very much a waste of important time that the opposition is allotted", but that in this case he felt the issue was important (*Hansard Vol. 147 No. 80,* 4933). This statement alone is intended to minimize the concerns of the opposition parties as generally being a waste of his time. In 2014 there were a total of 127 sittings in the House of Commons, with only 22 of those days designated as allotted days. Frequency analysis on the transcripts for 2014 revealed that the name 'Mike Wallace' only appeared in 68 of the 127 sittings during 2014, meaning he either didn't rise to speak or didn't attend the 59 other sittings. His participation in the house during 2014 puts his comment about 'wasted time' in perspective.

Wallace goes on to describe the following scenario in regards to subject of the motion; the 1.2 million requests for personal information:

> The vast majority of those investigations were agencies requesting voluntary co-operation. Before we go any further, it is voluntary co-operation. They ask and the service providers provide. They are not providing all the content of what an individual may be using or looking at through their IPs or service provider, whether it is a cellphone or the Internet, but they are providing basic address information such as name and address.
>
> A simple example would be this. The police could look in the phone book. They know where I live. I know who is on my street. I have lived there for 16 years. Police might come to my door and ask if so-and-so lives next door. I have to say "yes". I voluntarily provide that information and that is basically what has been asked for. I do not give the police permission to go into my neighbour's mailbox, open their mail, and read their mail. That is not the permission we are providing and that is being accessed here. (*Hansard Vol. 147 No. 80,* 4934)

Wallace's comment that he would "have to say yes" if the police asked about specific people living next door is false. The Supreme Court ruling of *R. v. Turcotte* states that the right to silence is protected by the Charter, even in a voluntary interaction with police (para. 52). While he may voluntary provide that information, he doesn't have to. When Robert Aubin of the NDP, asks for clarification from Wallace about the nature of the information being provided, Wallace reiterates that the disclosure of information by telecommunications companies is voluntary, he states:

> I would remind the House that this information that we are talking about has been provided voluntarily. Companies can refuse, if they feel so inclined. Then a warrant would be required for further investigation. (*Hansard Vol. 147 No. 80,* 4935)

Scott Andrews of the Liberal Party, becoming frustrated by Wallace's remarks, says that he is "missing the point" and asks if he would "give up his IP address voluntarily for the House if it is not such a big important piece of information" (*Hansard Vol. 147 No. 80,* 4935). Wallace responds with the following statement:

> If the police came to me and asked me who I called and what I said to them, I would be happy to provide it for them voluntarily because I have *nothing to hide*. I am not sure whether that would happen with my colleague from the other side.
>
> On the voluntary piece, I have no issue with that. However, I do understand that once we get into that, it is important that people have the right to privacy, to say, "No. If you want to see who I've talked to and what we've talked about, if you want to see what websites I'm looking at and the information that I'm passing back and forth using the Internet, yes, you do need, if that's your decision, a warrant to get that information". That is what is still and continues to be protected under the law. (emphasis added) (*Hansard Vol. 147 No. 80,* 4935)

This is an interesting statement by Wallace, most notably because when he is challenged by Andrews about providing his personal information, he responds by saying he has "nothing to hide". The 'nothing to hide' argument was discussed in Chapter 2. It depends on a narrow

interpretation of privacy as secrecy or concealment by framing the disclosure of personal information as a threat only when people are engaging in unlawful activities. Wallace questions whether Andrews would voluntarily provide his own personal information, which implies that if Andrews didn't, then he *would* have something to hide, which further implies his participation in criminal activity.

Law-abiding Canadians

Protecting the 'privacy rights' of 'law-abiding Canadians' is a common theme in this debate. The motion on which the debate has occurred is specifically concerned with the "indiscriminate disclosure of the personal information of law-abiding Canadians" (*Hansard Vol. 147 No. 80,* 4899), with Borg using the phrase four more times in her opening statement. She says that the vast amount of Canadians are law-abiding, and that her motion is "meant to counter the government's nefarious attempts to get information by the back door" (*Hansard Vol. 147 No. 80,* 4899). She goes on to say that "(l)aw-abiding citizens should be able to benefit from the Internet without the threat of being treated like common criminals" and that the government needs to be held accountable for spying on their own citizens (*Hansard Vol. 147 No. 80,* 4899).

Hon. Steven Blaney, the first CPC MP to speak to the motion, agrees, explaining that it is important for the government to be mindful of the balance between enforcing the laws and protecting national security, which ensures "that law enforcement has the tools it needs to do its job while law-abiding citizens continue to be free from any form of government harassment" (*Hansard Vol. 147 No. 80,* 4899).

Mathieu Ravignat of the NDP argues that privacy laws need to be strengthened, not weakened, in order to "take effective legal action against criminals without infringing on the rights of law-abiding Canadians and treating them like criminals" (*Hansard Vol. 147 No. 80,* 4913). Cleary of the NDP says almost the exact same thing a few minutes later (*Hansard Vol. 147 No. 80,* 4913). Angus of the NDP likens the 1.2 million requests for personal information to a "massive fishing expedition", asking why the government has "declared open season on the private rights of law-abiding Canadian citizens" (*Hansard Vol. 147 No. 80,* 4922). Later, Davies repeats the NDP's 'strengthen, not weaken' argument, by saying that "New Democrats believe that we can and should aggressively pursue criminals and punish them to the full extent of the law without treating law-abiding Canadians like criminals and violating their rights" (*Hansard Vol. 147 No. 80,* 4945).

Rob Clarke of the CPC echoes Blaney's statement about balance, saying that he wants to "set the record straight" by reassuring "all Canadians that our government always strikes an appropriate balance between giving law enforcement officials the tools they need to do their job and protecting the privacy of law-abiding Canadians" (*Hansard Vol. 147 No. 80,* 4950).

Fairclough suggests that in the analysis of the features present in a text, it is also important to consider what other choices might have been made in terms of the orders of discourse that the text draws upon (*Language and Power* 129). What is not included in a text may have just as much meaning as what is. The overwhelming message in the previous excerpts by both the government and the Official Opposition is that the privacy of law-abiding Canadians must be

protected, because violating a person's privacy is tantamount to treating them like a criminal.

This assertion is problematic for two reasons. First, if violating a person's privacy necessarily is treating them like a criminal, then why is there so little information about the nature of the 1.2 million requests for information made in 2011? It would stand to reason that a government so committed to supporting the needs of law enforcement would want to publicize the positive effects of a voluntary relationship between telecommunication companies and the police by providing statistics that show crime is declining. It seems like they are using the concept of voluntary disclosure to minimize their responsibility for instances when the sharing of information may have been unnecessary, while also denying that the information they are requesting is private at all, through the use of the phone book analogy.

Second, what is not being said in the repeated references to the privacy rights of law-abiding Canadians, is that non-law abiding citizens have privacy rights too. This was clearly articulated in *R. v. Spencer*, which ruled in favour of the privacy of a man who was downloading child pornography.

Furthermore, the Charter of Rights and Freedoms has a number of explicit rights that directly apply to people who have been charged and convicted of a crime, which means that the Charter applies to all citizens, not just the ones that abide by the law.

The last and final section of this chapter will focus on Fairclough's third stage of CDA, explanation. This stage will draw together observations from the previous analyses in order to draw conclusions about the meaning of privacy and how it is shaped by the social structure and relations of power in the House of Commons.

4.3 Explanation

Fairclough's final stage of CDA is again structured with guiding questions, although loosely. The first purpose of the explanation stage is to determine how relations of power at the situational, institutional, and societal levels shape the discourse under study (Fairclough *Language and Power* 175). The second purpose is concerned with uncovering the ideological character embedded in the cognition of the discourse participants (Fairclough *Language and Power* 175). And the third purpose involves an examination of the effect of the discourse on sustaining or transforming existing power relations (Fairclough *Language and Power* 175).

Relations of Power

The power relations that most visibly shape the discourse of privacy occur at the situational level, between the government and the opposition parties in the House of Commons. The entire structure of the system of parliamentary democracy is designed to concentrate power in the hands of the party who wins the highest number of seats in an election. The result is that the government who holds the majority has the clear advantage in a debate, not because they can speak more but because they have more votes. This has a direct effect on the entire legislative power in the House of Commons, though there are checks and balances at the levels of the Senate and the Governor General. Yet, an analysis of the discourse of Hansard is still of value, precisely because the structured nature of debate allows for the expression of different points of view. Because of the nature of the party system in the House, these view points tend not to vary from person to person, but rather from party to party. This was evinced in the last section through the appearance of very repetitive statements by members of both the CPC and the NDP. This repetition is a result of the ability of each party's Whip to enforce discipline among the members of the party.

The nature of the discursive practice of debate influences the relations of power between the discourse participants, but also at the level of the institution, in the relations between the House and the people they are elected to represent. The fact that motions, and ultimately legislation, must be considered and decided upon through the practice of debate constrains the types of issues that can be discussed. Anything that is brought up through the course of a debate must be able to withstand the practical argumentation required by virtue of the discourse type. Motions must be practical, affirmative, and actionable, leaving little opportunity to discuss issues in abstraction, such as ethics and philosophy. While there are other venues within the institution of Parliament to address such issues, such as reports by Standing Committees, the discourse type of debate constrains what can be discussed in the situational context of the House of Commons.

This has an impact on the societal relations of power between the institution of Parliament and the citizens of Canada. The legislative power of the House of Commons determines what may or may not be done in society. This power is enacted through the discursive practice of debate, which influences what types of issues can be discussed, which is further influenced by whichever party holds the majority in the House, which is influenced by the ability of certain people to occupy the social role of politician through getting elected.

The relations of institutional and societal power also extend across social orders of discourse. While Parliament is responsible for creating legislation, the courts are responsible for interpreting it. In terms of CDA, the discourse of legislation is produced by Parliament, but interpreted by the courts, which eventually leads to a further interpretation by Parliament. But the structures of these two institutions are very different. As it was discussed earlier in this section, the deliberative nature of parliamentary discourse is focused on using practical argumentation to make a decision about what ought to be done in a certain situation. This is entirely different from the nature of judicial discourse, which instead is focused on the defence or condemnation of someone's actions (Fairclough and Fairclough 90). While parliamentary discourse is forward-looking and normatively focused on decisions that will impact large groups of people, judicial discourse focuses on looking back on an event with the intent of determining what should be done about a specific individual or group. The entire structure of both the institutions of politics and justice are strongly influenced by their respective discursive practices, and these discursive practices are dramatically different. The interpretation of discourse is highly dependent on the cognition and ideology of the discourse participants, which is in turn influenced by the structure of the institution within which the discourse occurs. The interpretation of discourse across these two institutions will be influenced by each discourse participant's understanding of the nature of the institutions themselves, which in these two situations, may be very different.

The struggle for power between political and judicial orders of discourse is further evident in the ability of the court to effectively question the meaning of the legislation it is meant to enforce. In *R. v. Spencer*, Justice Cromwell pointed out a circularity in PIPEDA between s. 5(3) and s. 7(3)(c.1)(ii), where the interpretation of both sections relies on an understanding of the concept of a reasonable expectation of privacy. While the ruling does not change the legislation, it does set a strong legal precedent, which influences the results of any future interpretation of the law where the circumstances are similar. This has the effect of rendering that provision useless, as it is indefensible in terms of the courts, even though it remains in the legislation.

Societally, this process of production and interpretation of discourses across and between institutions has a direct effect on the relations of power between all the participants, which in the case of legislative and judicial power, is everyone in Canada. This is especially salient in terms of the differing abilities of people in navigating the complex and formal aspects of these institutions. Those who have had a reduced access to literacy acquisition will have the least power in a system defined by complex rules of formal language.

Ideology

Even in the disagreement between the Official Opposition and the government on the semantic difference between the 'warrantless disclosure' or the 'voluntary disclosure' of personal information, it is evident that both parties are operating under the narrow assumption of privacy *as* secrecy. While this is most clearly shown by the use of the phrase 'nothing to hide' in CPC MP Wallace's statement, it is also evident in the repeated references to 'law-abiding Canadians' by members of the of both the CPC and the NDP. This separation of Canadians into categories of 'law-abiding' and 'criminal' uncovers a hidden ideological discourse that

an individual should only expect privacy when they abide by the law. As it was discussed in Chapter 2, this narrow conception of privacy has deep implications for society, especially in terms of freedom of expression. Surveillance has a chilling effect on society, and the fact that 1.2 million requests were made for personal information in 2011 alone is indicative that the government, and the House as whole, has no ideological basis for the other dimensions of privacy, the most important of these being that an individual's privacy is inherently connected to their expectations of anonymity, regardless of whether or not they are abiding by the law. Throughout the course of the debate, parties from both sides of the House agreed that the police have the power to get a warrant when they have suspicions about criminal behaviour. It is unclear why they would need to compartmentalize the expectation of privacy within of certain groups of Canadians in order to allow law enforcement to use the tools that are already legally afforded to them.

This exchange, as well as the CPC comments about the Charter being responsible for the protection of personal information, exposes a deep misunderstanding about the nature of the Charter among all of the MPs who participated in the debate. While s. 8 of the Charter has been used in jurisprudence in support of privacy, it has not been declared a right. Not one MP pointed this out. Nor was Wallace's claim that he would 'have' to give information to the police, when s. 7 of the Charter has been declared by the Supreme Court as supporting the right to be silent in matters involving the police. The comments, and the fact that they weren't refuted, exposes an ideology in the House that rights only apply to people who abide by the law. This contradicts the very nature of the Charter, as it applies to all citizens of Canada. And, as it was already mentioned, there are numerous Charter rights that apply specifically to people who have been accused, charged, and convicted of a crime.

Sustaining Power

The discourse that there is a difference in the rights afforded to different groups of Canadians is harmful. The continual reference that privacy is a right afforded only to law abiding citizens creates a pervasive and influential hidden discourse, which serves to normalize the concept as a matter of common sense.

This marginalizes the perception of the privacy rights afforded to those who have been accused, convicted or charged with a crime, contributing to a social ordering of discourse that preferences the general rights of 'non-criminals', while diminishing the value of the rights of 'criminals'. This is despite the alternative discourse in the jurisprudence, such as *R. v. Spencer*, which maintains that the privacy interest of all citizens, despite their ability to 'abide by the law', is protected.

While the normative structure of the House of Commons is understood as a place where the law is the supreme authority, in reality, the MPs do not have a clear understanding of the law in terms of the protection of privacy, or for that matter, what is and isn't a right in Canada, and who those rights apply to.

The power in this discourse is in the representation. The ideological character is completely lost when all of the parties in the House maintain the discourse through the repeated references

of the relationship between 'privacy rights' and 'law-abiding Canadians'. The discourse of privacy in the House of Commons is relegated to the narrow definition of privacy as secrecy for those who abide by the law. The effect of this order of discourse affects not just the structure of the Parliament, but the structure of the institutions involved in justice and law enforcement, which in turn affects the cognition and ideology of everyone who comes into contact with those institutions. The more this discourse is represented as a matter of common sense, the harder it will be to change.

5 Conclusion

In order to have a reasonable expectation of privacy, the meaning of privacy must first be understood. While the privacy of personal information is protected in Canada by a number of federal statutes, none of them include a definition or explanation of the meaning of privacy.

Through a two-stage text analysis of all the parliamentary debates between the 39th and the 41st Parliaments, it was determined that privacy was narrowly defined by the House of Commons during that period as a 'right to secrecy for Canadians who abide by the law'.

Research Summary

This conclusion was drawn from the results of two complementary methods of text analysis as well a review of the privacy legislation, literature, and jurisprudence in Canada.

The review of the legislation, literature, and jurisprudence was primarily contained to documents pertaining to the federal level of governance in Canada, the House of Commons. The review determined that privacy, in terms of Canadian federal legislation such as the Privacy Act and PIPEDA, is overwhelmingly concerned with the protection of personal information, as it relates to its collection, use, disclosure, and destruction. While privacy is not a right in Canada, the Privacy Act has been considered to be a quasi-constitutional piece of legislation, which is a symbol of the importance of privacy and privacy legislation in a free and democratic society such as Canada. PIPEDA has been characterized as fundamental, but not quasi-constitutional. This review also summarized some of the major philosophical concepts regarding the importance of privacy to society, coming to the conclusion that a reasonable expectation of privacy amounts to a reasonable expectation of anonymity. Anonymity can be understood as the freedom of an individual to negotiate societal expectations, both in public and in private, while remaining free from identification.

The first method of text analysis processed the text electronically as a means of generating frequency and concordance data. The text was compiled into a corpus from the publication known as Hansard, which consists of the complete transcripts of the parliamentary debates in the House of Commons. The corpus was organized as two distinct parts: yearly, from 2006 - 2015 inclusive; and by Parliament and Session, starting with the 1st Session of the 39th Parliament and ending with the 2nd Session of the 41st Parliament. Using the coding language Python, information about the frequency of the word 'privacy' was determined and concordances were generated, which showed the context of 'privacy' at the level of the sentence.

The results of this first text analysis informed the selection of a specific debate for the second analysis, which was chosen as a result of the frequency of the phrase 'privacy rights'. This phrase had the highest relative frequency in 2014 compared to any of the other years in the corpus. The sitting of May 5, 2014 was chosen for analysis, again due to the fact that it had the highest relative frequency of the phrase 'privacy rights' compared to any other sitting in that year. The transcript was analyzed using Fairclough's method of Critical Discourse Analysis, which argues that language can only be understood within the context of its use. This requires

an interpretation and examination of the social structures, institutions, practices, roles, and relations that collectively led to the construction of the text under analysis. The analysis determined that the debate of May 5, 2014 was a representation of the political practice of parliamentary debate, which consists of political actors engaging in persuasive practical argumentation with the purpose of making a decision about a topic or situation. By nature, parliamentary debates are a struggle over power and meanings, as the constraints that exist due to the nature of the discourse type, notably the reliance on a majority vote, concentrate power in the hands of those who have the most physical representation in the institution of Parliament. Despite this imbalance of representation, which is organized in the House of Commons by ideological party, the results of this particular analysis determined that the MPs in this debate shared a common ideology regarding the meaning of privacy. This meaning will be discussed in the Key Findings section of this chapter.

This research is significant for two reasons. First, it showcases the interdisciplinary value of text analysis as a methodology with the successful integration of electronic and critical text analysis. Despite the assertion by Fairclough that the combination of electronic methods of text analysis and CDA contribute to the creation of "watered down criticism" (*Language and Power* 36), I strongly believe that a research project of this nature would not have been possible without the combination of both methods. Both methods of analysis are subject to the inherent biases of the researcher, and as long as that subjectivity is acknowledged and 'called out' by the researcher through the course of the both analyses, there is no danger in the combination of methods.

Second, at the point of publication, a study of this breadth and depth has yet to be done on the transcripts of the Canadian Hansard. One of the key motivations of CDA is to expose the orders of discourse that contribute to the reinforcement or maintenance of the unequal distribution of power in society as a means of inspiring change. I can only hope that this study, or studies like it, will have a subtle impact in this regard.

Since I have posted my data and my code online, other researchers can conduct their own analyses, without having to download all of the files from the House of Commons website or learn a lot of code. I have shared the files in their original format, XML, as well as in a plain text format, which has been processed to remove the XML formatting. The code is easily accessible for the purpose of scrutiny or reuse.

Key Findings

To build on Finestone's metaphor, privacy legislation in Canada really is a patchwork garden full of weeds (26), and the MPs responsible for tending the garden cannot even distinguish between the helpful plants and the invasive ones.

A 'Charter right to privacy'

This characterization stems from the analysis of the May 5, 2014 debate, where Conservative MPs continuously referred to a 'Charter right to privacy', even though no such right exists. None of the opposition MPs in the House that day attempted to refute this claim. While s. 8 of the Charter has been used successfully as a privacy defence, it only applies in the

case of the unreasonable disclosure of personal information where either the consent of the individual, or a warrant from the court has not been previously obtained. Referring to privacy in this way is categorically false, and while this was proven conclusively in only one debate, the repeated occurrences of the phrase 'privacy rights' throughout the entirety of the Hansard corpus suggests that May 5th was likely not an isolated event.

The definition of 'personal information'

This fundamental misunderstanding of the 'right to privacy' was compounded by the MPs inability to agree on the definition of personal information during the course of this particular debate. Despite the fact that personal information is generally defined in both the Privacy Act and PIPEDA to include "information about an identifiable individual" (PIPEDA, s. 2(1); Privacy Act, s. 3), the MPs spent a great deal of time quibbling about whether or not an IP address constituted 'basic subscriber information' in the way that a name or a phone number does, with some MPs using the analogy of 'phone book' to make their point. This is problematic for two related reasons. The first concerns the definition of personal information in the Privacy Act, and the second relates to the distinction between 'information about identity' and 'information that identifies'.

The extended definition of personal information in the Privacy Act includes a qualifying phrase specifying that even the name of an individual is protected as personal information if it appears with other personal information relating to the individual (s. 3(i) 'personal information'). What this means, in terms of the confusion around the meaning of basic subscriber information in the debate, is that the very fact that an IP address accompanied the name and phone number of an individual makes *all* of the information 'personal.' Because the IP address is related to an individual in a way that identifies them, the name, phone number, and IP address all equally deserve protection from disclosure. While the debate in question was generally on the topic of PIPEDA and Bill C-13, rather than the Privacy Act, any one of the MPs could have drawn on this definition as a point of clarification or to advance their argument. There were many occasions in this debate where MPs made reference to other pieces of legislation and Bills to advance their claims. The fact that none of them were aware of this important definition in a highly relevant piece of legislation speaks to a general lack of knowledge in the House about the meaning and intent of both of the Acts.

Related to this point is the distinction between 'information about identity' and 'information that identifies' (Slane and Austin 501). The reason the Privacy Act specifically calls out the relationship between an individual's name and other information that relates to that information, is because linked information identifies. While it is true that names and phone numbers are freely available in publications like the phone book, IP addresses are not, precisely because they have the potential to reveal a vast amount of other personal information about an individual in a way that a name or phone number cannot. This concept was brought up in the debate in terms of a quote by former Privacy Commissioner Cavoukian, but never fully articulated or debated (*Hansard Vol. 147 No. 80,* 4902).

It's important to note that the ruling in *R. v. Spencer* was about this very issue, and the judgment was made in favour of protecting personal information, which includes IP addresses,

from warrantless disclosure.

Much like the misinterpretation of the Charter, it is highly unlikely that the MP's confusion surrounding the definition of personal information was isolated to this single debate.

The 'hidden discourse' of privacy

This confusion speaks to a deeper undercurrent of ideological belief in the House of Commons that answers the question posed at the beginning of this thesis, which sought to determine the meaning of privacy as it is understood and used by MPs.

The key distinction between 'information about identity' and 'information that identifies' is anonymity. Anonymity is not the same as secrecy; it is not an argument for keeping every single piece of information about the self private through the act of concealment. Rather, anonymity involves the ability of individuals to experiment with thoughts and opinions without the risk of ridicule, shame, or punishment from others, regardless of whether they are in a public or private space (Westin 33-34). Neither is anonymity a cover for committing illegal acts. The Criminal Code, the Privacy Act, and PIPEDA all contain provisions that allow for the lawful disclosure of personal information when a crime has not only occurred, but is suspected to occur.

The continued reference to the 'privacy rights' of 'law-abiding Canadians' by all Members of the House during this debate exposes a major ideological discourse which implies that only Canadians who abide by the law deserve privacy. Yet the protections afforded by both pieces of federal privacy legislation, as well as the Charter of Rights and Freedoms, apply equally to all Canadians, whether or not they engage in criminal activities. The implication that criminals do not deserve privacy relies on the assumption that criminals only want privacy because they have something to hide. This means that MPs, at least in the context of their role of politician in the House of Commons, subscribe ideologically to the narrow definition of privacy *as* secrecy.

The marginalization of criminals and suspected criminals -- who are already in a drastically reduced position of power in society due to legal proceedings, imprisonment, punishment, and shame -- is not even the worst part about this discourse. The problem with defining privacy as secrecy, rather than as anonymity, is that it suppresses the power and autonomy of all citizens in Canadian society by implying that an individual's need for privacy is not necessary when they have nothing to hide (Solove 746-747). Westin argues that privacy is essential to the development of a person's complete and unique sense of self, but that this depends almost entirely on the ability to anonymously experiment with thoughts and ideas before testing them out in society or discarding them (33-34).

A lack of anonymity, whether real or implied by discourse, ultimately has a 'chilling effect' on society as a whole, where people are more likely to conform to societal expectations rather than freely express their thoughts, viewpoints, and political beliefs (Solove 765; Task Force 18). The definition of privacy as secrecy is contrary to the quasi-constitutional status afforded to the Privacy Act by the Supreme Court, which stated that the Act should serve as a "reminder of the extent to which the protection of privacy is necessary to the preservation of

a free and democratic society" (*Lavigne v. Canada* 789).

This is yet another serious example of the MPs fundamental misinterpretation and misunderstanding of the legislative power they wield, which is deeply troubling in that the stated purpose of a parliamentary democracy holds that the law is the supreme authority.

Limitations

The limitations of this research fit into two distinct categories: technical and theoretical. The technical limitations concern my ability to write code. The sheer size of the corpus, almost 69 million words, meant that web-based tools or programs were just not able to process the text. This resulted in my learning the coding language Python as I conducted the research. I made a lot of mistakes along the way, which resulted in several false starts and required many reinterpretations of the results. Due to size of the corpus, and my novice understanding of code, some of the data that was generated needed a substantial amount of cleaning before it could be considered for analysis. This applies primarily to the generation of collocational statistics, which ended up being the least necessary and most time consuming method of text analysis in the course of my research; consisting of the only data that I ultimately ended up not using. Since I was already interested in investigating a specific word, the collocational statistics merely confirmed the trends already discovered by the frequency statistics and concordances. In this regard I agree with Wermter and Hahn, who argue that simplicity is a good approach when it comes to text analysis (785); the most compelling trends in this research were the basic frequencies, and they were also the easiest to generate.

The theoretical limitation of this research concerns the inherent subjectivity of text analysis as a research method. Text does not simply come into being, nor does it provide an objective representation of reality, it is understood and influenced by the individual cognition of the researcher, the context within which it was originally created, and the relationship between the researcher, their cognition, and their interpretation of the text to its context. Both computerized text analysis and Critical Discourse Analysis are subject to the biases and preconceptions of the researcher; this begins with the selection of a text or text collection, continues through the choice and application of methods, and ends by strongly influencing the interpretation and discussion of the results. The theoretical intention of the researcher is present at every stage (Stubbs, *Text and Corpus Analysis* 154) and more than one theoretical intention can be applied to the same research problem (Kuhn 76).

Specifically, the use of CDA as a methodology implies that the researcher is strongly influenced by personal ideology. The aim of CDA is to critically analyze the ways in which language contributes to the struggle for power in society, which means that the researcher believes that power imbalances are something that requires criticism. If I was not concerned about my own need for informational privacy, it is unlikely that I would have chosen to research it. Similarly, if I was not concerned about the implications of Bill C-13 in terms of warrantless access of personal information, I would have chosen another body of text to analyze. The fact that the first stage of text analysis pointed to trends that I deemed worthy of further investigation confirms that I suspected the trends would exist.

Despite these limitations, the nature of text analysis, especially in terms of electronic methods, allows for the reproduction, examination, and critique of the work by others. This is the reason I have made my data and code publicly available. Publishing data and code serves the dual purpose of opening up my analysis to criticism and review, and promoting the application of text analysis as a methodology for future research.

Potential for future research

The most obvious potential for future research in terms of this specific collection of text would be a deeper investigation of some of the other trends identified by this research. While 2014 was an interesting year in terms of the frequency of privacy, so was 2011, and it would make sense to continue the CDA at that point in the text. Hansard continues to be published online, and it would be interesting to see if the House of Commons comprised of a new government compares to the previous government in terms of the discourse of privacy. This will require more time to pass, as the 1st Session of the 42nd Parliament has yet to be prorogued.

The public availability of the data and the code lends itself to the investigation of other topics, and another researcher could pick this up quite easily. The code has been published in iPython Notebook, which is a format that allows people with all levels of coding literacy to use the code, involving only a minimum degree of setup on their own computers. This means that the code can continue to be used in the analysis of the Hansard corpus, but also for other bodies of text. In this regard, it would be interesting to analyze the jurisprudence discussed in this research in order to do a comparative analysis of the difference between judicial and parliamentary discourse. This is an area where collocational statistics may have more relevance, although I will continue to advocate for simplicity, rather than complexity in the selection of methods for text analysis.

Interest in the acquisition of coding literacy among librarians and scholars in the humanities and social science disciplines is increasing. The structure and methodology of this thesis contributes to the growing body of interdisciplinary research that studies text and discourse from the dual perspectives of close and distant reading.

Final Thoughts

Distant reading, as it is described by Moretti, involves stepping so far back from a collection of text that it effectively disappears and cannot be traditionally read (57). From that distance, a unit of analysis can be defined and followed throughout the entirety of the collection (Moretti 61-62). In this case of this research, the unit of analysis was focused on a single word: ‘privacy’, which was then followed from the beginning to the end of the Hansard corpus. Metaphorically, the word rose from the text like a beacon, occurring exactly 6,478 times in a sea of almost 69 million other words. By employing the methods of text analysis, this distant reading instantly revealed patterns of frequency and use that would have otherwise required months to uncover by hand. These distinct areas of interest enabled a focused reduction of the distance, which allowed phrasal patterns (concordances) to emerge.

To paraphrase Adolphs, the discovery of frequencies and phrasal patterns provided a

way into the text that was informed by the text itself (19). The close reading necessary for CDA was performed on a small selection of text that was most representative of the trends uncovered by the distance. Mautner argues that the method moving from a large body of text to a small selection helps to reduce some of the bias from CDA (123), much like the limitations discussed above. I believe that the distance does not reduce bias in terms of influencing the initial selection of text, which is her argument, but in the ability of the researcher to make a stronger critical claim *as a result* of the distance.

While nothing can be conclusively 'proven' by either method of text analysis, my critical claim that privacy is narrowly defined in the House of Commons as a 'right to secrecy for Canadians who abide by the law' is supported by the results of the distant reading, which uncovered clusters of phrases and patterns of word use that spanned the entire corpus. Furthermore, since I have openly provided both the data and the code, those who refute my claim can come to their own conclusions through the replication or advancement of my work.

Works Cited

Adolphs, Svenja. *Introducing Electronic Text Analysis: A Practical Guide for Language and Literary Studies*. London: Routledge, 2006.

Austin, Lisa M. "Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State". *Law, Privacy, And Surveillance In Canada In The Post-Snowden Era*. Ed. Michael Geist. Ottawa, Ontario: University of Ottawa Press, 2015.

Bailey, Jane. "Framed by Section 8: Constitutional Protection of Privacy in Canada." *Canadian Journal of Criminology and Criminal Justice* 3 (2008): 279.

Baker, Paul. *Using Corpora in Discourse Analysis*. London; New York: Continuum, 2006.

Bayley, Paul. *Cross-Cultural Perspectives on Parliamentary Discourse*. Amsterdam: J. Benjamins Pub. Co, 2004.

Bill C-13 Protecting Canadians from Online Crime Act. *Statutes of Canada, 2014, c. 31.* Canada. Department of Justice. 2014.

Bill S-4 Digital Privacy Act. *Statutes of Canada, 2015, c. 32.* Canada. Department of Justice. 2013.

Bird, Steven, Ewan Klein, and Edward Loper. *Natural Language Processing with Python*. O'Reilly Media, 2009.

Burrows, John. "Textual Analysis." *A Companion to Digital Humanities*. Ed. Susan Schrelbman, Ray Siemens, and John Unsworth. Oxford: Blackwell, 2004.

Criminal Code. *Revised Statutes of Canada, c. C-46*. Canada. Department of Justice. 1985.

Danielsson, Pernilla. "Automatic Extraction of Meaningful Units from Corpora: A Corpus-Driven Approach Using the Word Stroke." *International Journal of Corpus Linguistics* 8.1 (2003): 109–127.

Dept. of Communications, and Dept. of Justice. *Privacy and Computers; a Report of a Task Force Established Jointly by Dept. of Communications Dept. of Justice*. Ottawa: Information Canada, 1972.

Dijk, Teun A. van "Critical Discourse Analysis." *The Handbook of Discourse Analysis.* Ed. Deborah Schiffrin, Deborah Tannen and Heidi E. Hamilton. Oxford: Blackwell, 2003.

--- "What Is Political Discourse Analysis?" *Belgian Journal of Linguistics* 11.1 (1997): 11.

Eastmond v. Canadian Pacific Railway. 2004 FC 852. (CanLII).

Fairclough, Norman, and Isabela Fairclough. *Political Discourse Analysis*. New York : Routledge. 2012.

Fairclough, Norman. *Language and Power*. 3rd ed. New York : Routledge. 2015.

--- "The Discourse of New Labour: Critical Discourse Analysis." *Discourse as Data : A Guide for Analysis.* Ed. Margaret Wetherell, Stephanie Taylor and Simeon Yates. London; Thousand Oaks, Calif.: SAGE, 2001.

Finestone, Sheila. *Privacy, Where Do We Draw the Line? : Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities*. Ottawa : Public Works and Government Services Canada-Publishing, 1997.

Floridi, Luciano. *Information: A very short introduction*. Oxford; New York: Oxford University Press, 2010.

--- "A Defence of Informational Structural Realism." *Synthese: An International Journal for Epistemology, Methodology and Philosophy of Science* 161.2 (2008): 219–253.

--- "Foundations of Information Ethics." *The Handbook of Information and Computer Ethics*. Ed. Kenneth Einar Himma and Herman T. Tavani. Hoboken, N.J. : Wiley, 2008.

--- "The Digital Revolution." *Philosophy and Computing : An Introduction.* London: Routledge, 1999.

Frawley, William J., Gregory Piatetsky-Shapiro, and Christopher J. Matheus. "Knowledge Discovery in Databases: An Overview." *AI Magazine* (1992): 57.

Gramsci, Antonio. *Selections from the Prison Notebooks of Antonio Gramsci.* Trans. Quintin Hoare and Geoffrey Nowell-Smith. New York: International Publishers, 1971.

Gratton, Eloise. "New Requirements Of The Digital Privacy Act (Bill S-4)." *Mondaq Business Briefing.* 22 Jun 2015.

Gries, Stefan Th. "Useful Statistics for Corpus Linguistics." *A Mosaic of Corpus Linguistics: Selected Approaches*. Ed. Aquilino Sànchez and Moisés Almela. Frankfurt am Main: Peter Lang, 2010. 269–91.

Guide to Making Federal Acts and Regulations. Ottawa: Privy Council Office, 2001.

Hajič, Jan. "Linguistics Meets Exact Sciences." *A Companion to Digital Humanities*. Ed. Susan Schrelbman, Ray Siemens, and John Unsworth. Oxford: Blackwell, 2004.

Harris, Sandra. "Being Politically Impolite: Extending Politeness Theory to Adversarial Political Discourse". *Discourse and Society* 12.4 (2001): 451-472.

Hennessey, Karen. *Response to Request for General Information from Canadian Wireless Telecommunications Association (the "CWTA") Members*. 14 December 2011. https://www.scribd.com/document/221023222/Telecom-Disclosures

Hockey, Susan. "The History of Humanities Computing." *A Companion to Digital Humanities*. Ed. Susan Schrelbman, Ray Siemens, and John Unsworth. Oxford: Blackwell, 2004.

House of Commons Debates, 41st Parl, 1nd Sess, 146.79 (13 February 2012): 5163-5231.

House of Commons Debates, 41st Parl, 2nd Sess, 147.80 (5 May 2014): 4889-4960.

House of Commons. Standing Committee on Access to Information, Privacy and Ethics. *Proposed Immediate Changes to the Privacy Act.* 39th Parl. 2nd Sess. Meeting No. 30. (29 April 2008).

Howard-Hill, T. H. *Literary Concordances : A Guide to the Preparation of Manual and Computer Concordances*. London; New York: Pergamon, 1979.

Hunston, Susan. *Corpora in Applied Linguistics*. Cambridge: Cambridge University Press, 2002.

--- "Semantic Prosody Revisited." *International Journal of Corpus Linguistics* 12.2 (2007): 249–268.

Kuhn, Thomas S. *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press, 1996.

Lavigne v. Canada (Office of the Commissioner of Official Languages). 2002 SCC 53. (Lexis).

Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA). Ottawa, Ont.: Office of the Privacy Commissioner of Canada, 2008.

LEGISInfo. "Bill C-30 An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts". *House Government Bill*. 41st Parl. 1st Sess. (14 Feb 2014).

Legislative Services Branch. "Personal Information Protection and Electronic Documents Act." n.p., 23 June 2015.

Library of Parliament. "Fixed-date Elections in Canada". *ParlInfo*. http://www.lop.parl.gc.ca/ParlInfo/compilations/provinceterritory/provincialfixedelections.aspx

Library of Parliament. "Parliaments". *ParlInfo*. http://www.lop.parl.gc.ca/ParlInfo/Lists/Parliament.aspx

Library of Parliament. "Party Discipline and Free Votes". *Topical Information for Parliamentarians* TIPS-81E (13 Jul, 2006): 1-3.

Mautner, Gerlinde. "Checks and Balances: How Corpus Linguistics Can Contribute to CDA." *Methods of Critical Discourse Analysis*. Ed. Ruth Wodak and Michael Meyer. Los Angeles ; London: SAGE, 2009. 122–142.

McEnery, Tony, and Andrew Hardie. *Corpus Linguistics: Method, Theory and Practice*. Cambridge; New York: Cambridge University Press, 2012.

McEnery, Tony, Richard Xiao, and Yukio Tono. *Corpus-Based Language Studies : An Advanced Resource Book*. London; New York: Routledge, 2006.

McInerney v. MacDonald. [1992] 2 SCR 138. (Lexis)

McIsaac, Barbara, Rick Shields, and Kris Klein. *The Law of Privacy in Canada*. Toronto : Thomson Reuters, 2000.

McKee, Alan. *Textual Analysis: A Beginner's Guide*. London: SAGE Publications Ltd, 2003.

McKenzie, D. F. *Bibliography and the Sociology of Texts*. Cambridge, U.K.: Cambridge University Press, 1999.

Mill, John Stuart. *On Liberty*. London : Penguin, 2010.

Mollin, Sandra. "The Hansard Hazard: Gauging the Accuracy of British Parliamentary Transcripts." *Corpora* 2.2 (2007): 187–210.

Moretti, Franco. "Conjectures on World Literature." *New Left Review* 1 (2000): 54–68.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris : Organisation for Economic Co-operation and Development. 2002.

Office of the Privacy Commissioner of Canada. "Your Guide to PIPEDA The Personal Information Protection and Electronic Documents Act." Apr. 2009.

--- "Proposed Immediate Changes to the Privacy Act: Appearance before the Standing Committee on Access to Information, Privacy and Ethics." April 29, 2008.

--- *The Case for Reforming the Personal Information Protection and Electronic Documents Act*. Ottawa, Ontario: Office of the Privacy Commissioner of Canada, 2013.

--- "Submission: Bill S-4, An Act to Amend the Personal Information Protection and Electronic Documents Act and to Make a Consequential Amendment to Another Act." n.p., 14 June 2014.

Olmstead v. United States, 277 U.S. 438. 1928. *Supreme Court of the United States.*

Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives. *Statutory Orders and Regulations, 2006-355*. Canada. Department of Justice. 2006.

O'Brien, Audrey, and Marc Bosc, eds. House of Commons Procedure and Practice. Ottawa : House of Commons ; Montréal : Éditions Yvon Blais, 2009.

Parliament of Canada. "Business of Supply." *Compendium of Procedure*. N.p., Oct. 2015.

--- "Debates (Hansard)." *Compendium of Procedure*. N.p., Apr. 2013.

Personal Information Protection and Electronic Documents Act. *Statutes of Canada, 2005, c. 5.* Canada. Department of Justice. 2005.

Privacy Act. *Revised Statutes of Canada, 1985, c. P-21.* Canada. Department of Justice. 1985.

R. v. Dyment. [1988] 2 SCR 417. (Lexis).

R. v. Plant. [1993] 3 SCR 281. (Lexis).

R. v. Spencer. 2014 SCC 43. (Lexis).

R. v. Turcotte. 2005 SCC 50. (Lexis).

Robertson, James R. "Television and the House of Commons." *Library of Parliament Parliamentary Information and Research Service* BP-242E (Sep 2005): 1-19

Schabas, William A. "Canada and the Adoption of the Universal Declaration of Human Rights." *McGill Law Journal* 2 (1997): 403.

Schwab, Sandra. *Adding Context to Word Frequency Counts*. mediagestalt/Adding-Context: v1.0 [Code]. 2016. http://doi.org/10.5281/zenodo.154735.

--- *Concordance Output.* mediagestalt/Concordance-Output: v1.0 [Code]. 2016. http://doi.org/10.5281/zenodo.154733.

--- *Counting Word Frequencies.* mediagestalt/Counting-Word-Frequencies: v1.0 [Code]. 2016. http://doi.org/10.5281/zenodo.154736.

Shannon, Claude Elwood, N. J. A. Sloane, and A. D. Wyner. Claude Elwood Shannon. *Collected Papers*. New York: IEEE Press, 1993.

Simpson, Richard. "Process for the Determination of 'Substantially Similar' Provincial Legislation by the Governor in Council". *Canada Gazette, Part I* 136.31 (2002): 2371-2418.

Sinclair, John. *Corpus, Concordance, Collocation*. Oxford: Oxford University Press, 1991.

--- *Reading Concordances : An Introduction*. London; New York: Pearson/Longman, 2003.

--- *Trust the Text : Language, Corpus and Discourse*. Ed. Ronald Carter. London; New York: Routledge, 2004.

Slane, Andrea, and Lisa M. Austin. "What's in a Name - Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations." *Criminal Law Quarterly* 4 (2011): 486.

Slembrouck, Stef. "The Parliamentary Hansard 'verbatim' Report: The Written Construction of Spoken Discourse." *Language & Literature* 1.2 (1992): 101.

Snowden, Edward. "Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU's Jameel Jaffer. AUA." *Reddit*, 21 May 2015. https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/

Solove, Daniel J. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review* 4 (2007): 745-772.

Sopinka, John. "Freedom of Speech and Privacy in the Information Age". Symposium on Free Speech and Privacy in the Information Age. University of Waterloo, Waterloo, ON. 26 Nov 1994. Keynote Address.

Stefanick, Lorna. *Controlling Knowledge : Freedom of Information and Privacy Protection in a Networked World*. Edmonton: AU Press, Saint-Lazare, Quebec : Canadian Electronic Library, 2011.

Stoddart, Jennifer. "An Overview of Canada's New Private Sector Privacy Law--The Personal Information Protection and Electronic Documents Act". 1 Apr 2004. Online Address.

Stubbs, Michael. *Text and Corpus Analysis: Computer-Assisted Studies of Language and Culture*. Oxford, UK; Cambridge, Mass., USA: Blackwell Publishers, 1996.

--- *Words and Phrases : Corpus Studies of Lexical Semantics*. Oxford; Malden, Mass.: Blackwell Publishers, 2001.

--- "On Texts, Corpora and Models of Language." *Text, Discourse and Corpora : Theory and Analysis*. Ed. Michael Hoey. London: Continuum, 2007. 127-161.

Sullivan, Ruth. *Sullivan on the Construction of Statutes*. 6th Edition. Markham, Ontario : LexisNexis Canada Inc., 2014.

Taylor, Stephanie. "Locating and Conducting Discourse Analytic Research." *Discourse as Data : A Guide for Analysis.* Ed. Simeon Yates, Stephanie Taylor, and Margaret Wetherell. London; Thousand Oaks, Calif.: SAGE, 2001.

Telecommunications Act. *Statutes of Canada, 1993, c. 38.* Canada. Department of Justice. 1993.

Teubert, Wolfgang. "My Version of Corpus Linguistics." *International Journal of Corpus Linguistics* 10.1 (2005): 1–13.

Thacker, Blaine. *Open and Shut : Enhancing the Right to Know and the Right to Privacy : Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act*. Ottawa: Queen's Printer for Canada, 1987.

Therrien, Daniel. "Letter to the Standing Committee on Access to Information, Privacy and Ethics". 22 Mar. 2016.

Tognini-Bonelli, Elena. *Corpus Linguistics at Work*. Amsterdam: J. Benjamins, 2001.

United Nations General Assembly. "International Covenant on Civil and Political Rights." *Treaty Series* 999 (1966): 171.

Universal Declaration of Human Rights : 60th Anniversary Special Edition, 1948-2008. New York: United Nations Dept. of Public Information, 2007.

Vedder, Anton. "KDD: The Challenge to Individualism." *Ethics and Information Technology* 1.4 (1999): 275–281.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4.5 (1890): 193–220.

Wermter, Joachim, and Udo Hahn. "You Can't Beat Frequency (Unless You Use Linguistic Knowledge) - A Qualitative Evaluation of Association Measures for Collocation and Term Extraction." *Annual Meeting - Association for Computational Linguistics* (2006): 785–792.

Westin, Alan F. *Privacy and Freedom*. New York, Atheneum, 1967.

Yates, Simeon. "Researching Internet Interaction: Sociolinguistics and Corpus Analysis." *Discourse as Data : A Guide for Analysis*. Ed. Simeon Yates, Stephanie Taylor, and Margaret Wetherell. London; Thousand Oaks, Calif.: SAGE, 2001.

Appendices

1 - Letter to former Privacy Commissioner Jennifer Stoddart in response to her request for information from the Canadian Wireless Telecommunication Association, 14 December, 2011

gowlings montréal · ottawa · toronto · hamilton · waterloo region · calgary · vancouver · moscow · london

PRIVACY COMMISSIONER RECEIVED DEC 15 2011 REÇU COMMISSAIRE VIE PRIVÉE

Karen E. Hennessey
Direct 613-783-8804
Direct Fax 613-788-3581
karen.hennessey@gowlings.com
File No. 02379950

December 14, 2011

PRIVATE AND CONFIDENTIAL

Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3

ATTN: Jennifer Stoddard

Dear Ms. Stoddard:

Re: Response to Request for General Information From Canadian Wireless Telecommunications Association (the "CWTA") Members

We are acting for the CWTA.

We write further to the Office of the Privacy Commissioner of Canada's ("**OPC**") request, which we understand was sent to twelve Canadian service providers asking for specific information about lawful access service in Canada.

A number of the service providers solicited by OPC are members of the CWTA. The CWTA members have expressed concern with providing the requested information on a company by company basis. After confirming with the OPC that they would accept information submitted on an aggregate basis, on September 14, 2011, the chair of the CWTA/ITAC Lawful Access Policy Committee, Bill Abbott, wrote to certain telecommunication service providers and requested that they submit their responses directly to Gowling Lafleur Henderson LLP for the assembly of a confidential aggregate report.

We have therefore agreed, as independent counsel for CWTA, to aggregate the responses received and provide a report in a format where quantitative and qualitative responses cannot be attributed to any one provider. We are bound to keep all company responses confidential.

We have received a response from nine providers. These providers provide wireline and wireless telephone service as well as retail and wholesale internet access service. As a group they represent a substantial proportion of Canada's telecommunications customer connections.

gowlings

Please find attached as Appendix A hereto, the aggregated response to the OPC's general questions concerning lawful access. We note that this Appendix A only provides a subset of the actual lawful requests and is based on nine Canadian providers.

Yours very truly,

GOWLING LAFLEUR HENDERSON LLP

Karen E. Hennessey

cc: Canadian Wireless Telecommunications Association

OTT_LAW\ 3000664

Appendix A:

Aggregated Response to the Office of the Privacy Commissioner Questions

Concerning Lawful Access

These responses have been aggregated and are being provided to the OPC, in accordance with the letter from Gowling Lafleur Henderson LLP dated December 14, 2011.

No.	Question	Company Response
1a	Approximately how many data requests from government authorities does your organization receive annually, on average?	Aggregate Average Annual Requests: 1,193,630 [1, 2] 1. This number includes an aggregation of responses from nine providers. 2. One provider provided the number of responses rather than the number of requests.
1b	Similarly, approximately how many users or accounts are subject to disclosure to authorities in response to a valid request? ***Explanatory Note (This question is difficult to answer. CNA requests usually correspond one request to one account/customer whereas Non-CNA requests may cover many accounts/customers.)***	Aggregate users and accounts subject to disclosure: 784,756 [1, 2, 3, 4,] 1. This total only includes three providers as five providers were unable to provide this information. 2. One provider replied that the average number of subscribers per request was 1.74. 3. One provider noted that all accounts are subject to disclosure with a valid request. 4. One provider replied that it cannot accurately determine the number of users and accounts subject to disclosure. Customer name and address requests usually correspond one request to one account/customer. Non-customer name and address requests may cover many accounts/customers.
2	Like some organizations, do you make these figures available to the public in any form?	No. [1] 1. One provider noted that it was recently required to provide a list of dates, times and information to a customer related to information released to the LEA in response to a privacy complaint from the customer.
3a	Do you keep internal, aggregate statistics on the types of requests you receive (such as production orders and emergency requests) and the kinds of information requested (e.g. subscriber records, non-content or transactional data,	Yes. [1, 2, 3, 4, 5, 6] 1. One provider noted that the numbers represent approximate numbers of requests received by law enforcement and government agencies of all levels nationally. In some cases, duplication and overlap may occur. For example, if a request is received to provide a name and address on a single account from

1

	communications content, location information customer look-ups, location data, emergency requests, wiretap requests, production orders)?	5 different law enforcement and government agencies, this is treated as five separate requests. Should the same request be submitted several times over the course of the year by the same law enforcement agency this is treated as an individual request. Such duplications are not tracked by the provider. Statistics pertaining to search warrants, production orders, government agency requirement letters and customer authorized third party disclosures (to government agencies or law enforcement) are tracked according to the number of customer files created in response to these disclosures, and not the number of actual authorizations received. For example, a single production order can require the production of records associated with 10 individual telephone numbers. This production order would be tracked as 10 requests. 2. One provider noted that statistics relating to requests for customer information, emergency requests, wiretap requests, and court orders received are kept at a high level of security for internal use only. 3. One provider noted that statistics relating to requests for customer information, emergency requests, wiretap requests, and Court Orders are kept at a high security level for internal use only. 4. One provider noted that it tracks the type of request, but not the kind of information requested. 5. One provider tracks the types of orders (production warrants, court orders, registered owner etc.) in its database system. The system records what is required from each order, such as CDR, text, tower, subscriber and information. This provider also keeps records of all lawful intercept warrants and orders in its database system. However, while certain statistics can be extracted from this database, it would require considerable manual effort as there are no existing reports. In addition, this data is classified as restricted information and cannot be disclosed without proper authorization. 6. One provider only tracks court orders on a monthly basis by province.
3b	If so, would you be willing to provide a copy of this information?	No.

4	If your enterprise uses Deep Packet Inspection equipment or software, have you used it in response to a request from federal authorities?	Two providers responded "Yes".[1] Five providers replied "No".[2, 3] Two providers did not provide a response to the question asked.
		1. One provider noted that it uses Deep Packet Inspection equipment for the limited use of decoding packets for source and destination routing information to facilitate delivery of Part 6 data delivery on Internet target interception. There is no packet inspection and analysis done. 2. One provider noted that it does not use Deep Packet Inspection equipment or software for the purposes of responding to requests from federal authorities. Interception of communications over data networks is accomplished by sending what is essentially a mirror image of the packet data as it transits the network of data nodes. This packet data is then sent directly to the agency who has obtained lawful access to the information. Deep packet inspection is then performed by the law enforcement agency for their purposes. 3. One provider noted that it commenced using Deep Packet Inspection equipment, in a lab environment in the beginning of Sept 2011, set to launch in its production environments in mid-October. It is intended to be used for traffic management purposes only.
5	Like some organizations, do you notify your customers, when the law allows, that their information has been requested, thus giving them an opportunity to contest the request in court?	No.
6a	Like some organizations, do you currently seek reimbursement for the cost of complying with these requests?	(a) Eight providers replied "Yes".[1, 2, 3, 4, 5, 6, 7] (b) One provider replied "No".

3

		1. One provider replied that it seeks reimbursement for the costs of complying with certain types of requests. Those include disclosure of customer name and address where judicial authorization does not exist and interception of communications. 2. One provider noted that its charges depend on the type of information requested. It provides assistance on a best efforts basis with cost recovery billing for lawful intercepts and technical assistance. It notes that some LEA's have refused to pay where the request is authorized by a court. There is no charge to LEA for emergency support, other than applicable levies for E911 tariffs. 3. One provider replied that LEA's are billed. 4. One provider replied that they seek reimbursement only for lawful intercepts at this time. 5. One provider bills agencies for establishing connections and their usage of telecommunication services on part 6 authorizations. These charges are based on cost recovery estimates. 6. One provider charges for CNAs and warrants which LEAs do not typical pay for. This provider also charges labour and facilities used for intercepts and notes that LEA's typical pay these charges. 7. One provider replied that they seek reimbursement only where costs are significant.
6b	If so, do federal authorities pay their bills in a prompt manner?	(a) Eight providers replied generally yes, with exceptions.[1] (b) This question is not applicable to the provider who replied "No" in Section 6 above.
		1. The general consensus was that the providers do not usually have any problems getting reimbursed but most providers also noted that there have been some difficulties with certain municipal police forces which refuse to reimburse the provider for their costs of complying with the requests.

4

6c	If not, what steps if any have you taken in order to obtain payment (such as terminating wiretaps and withholding data)?	(a) Six providers provided their payment process.[1, 2, 3, 4] (b) Three providers responded "Not Applicable."
		1. One provider noted that it has been provided with an explanation that they are awaiting Legislation compelling them to pay for warranted information, so this provider (at this time) takes no action to collect. 2. One provider replied that it still responds within a reasonable timeframe and at a minimum, as required by law. 3. One provider noted that it proceeds to take informal steps. 4. Three providers replied that at this time they do not take any of the measures as described in order to obtain recuperation of such costs in the event a law enforcement agency refuses to reimburse it for its costs.
7	Like some organizations, do you make a schedule of these tariffs or fees available to the public?	(a) Seven providers provided a reply with an explanation. [1, 2, 3, 4, 5] (b) Two providers replied "Not Applicable".
		1. One provider noted that they make available only to the extent there is a CRTC approved tariff. 2. Two providers noted that it complies with its general tariff on this issue. 3. Two providers noted that it does not make available to the general public, schedules of tariffs and fees associated with recoverable costs related to disclosures to law enforcement and government agencies. 4. One provider noted that this does not currently apply to its exchange of services. 5. One provider replied that it does not make its schedule of tariffs or fees available to the public, but does provide to Enforcement and Government Agencies.

2 - Speakers and number of speeches during the House of Commons Debate on 5 May 2014

Name	Riding	Province	Affiliation	# of speeches	Title
Mr. David Wilks	Kootenay Columbia	BC	CPC	7	
Ms. Roxanne James	Scarborough Centre	ON	CPC	6	Parliamentary Secretary to the Minister of Public Safety and Emergency Preparedness
Mr. Blake Richards	Wild Rose	AB	CPC	4	
Mr. Dave Van Kesteren	Chatham-Kent Essex	ON	CPC	4	
Mr. Rob Clarke	Desnethé Missinippi Churchill River	SK	CPC	4	
Hon. Steven Blaney	Bellechasse Les Etchemins Lévis	QC	CPC	3	Minister of Public Safety and Emergency Preparedness
Mr. Colin Carrie	Oshawa	ON	CPC	3	Parliamentary Secretary to the Minister of the Environment
Mr. Mike Wallace	Burlington	ON	CPC	3	
Hon. Michelle Rempel	Calgary Nose Hill	AB	CPC	2	Minister of State (Western Economic Diversification)
Mr. Paul Calandra	Oak Ridges Markham	ON	CPC	1	Parliamentary Secretary to the Prime Minister and for Intergovernmental Affairs
Mr. Daryl Kramp	Prince Edward Hastings	ON	CPC	1	
Ms. Elizabeth May	Saanich Gulf Islands	BC	GP	1	
Mr. Scott Andrews	Avalon	NL	LIB	9	
Mr. Kevin Lamoureux	Winnipeg North	MB	LIB	7	
Hon. Wayne Easter	Malpeque	PEI	LIB	1	
Mr. Sean Casey	Charlottetown	PEI	LIB	1	
Mr. Charlie Angus	Timmins James Bay	ON	NDP	9	
Ms. Charmaine Borg	Terrebonne Blainville	QC	NDP	8	
Mr. Don Davies	Vancouver Kingsway	BC	NDP	5	
Mr. Robert Aubin	Trois-Rivières	QC	NDP	5	
Mr. Ryan Cleary	St. John's South Mount Pearl	NL	NDP	4	
Mr. Dany Morin	Chicoutimi Le Fjord	QC	NDP	3	
Mr. Mathieu Ravignat	Pontiac	QC	NDP	3	
Mr. Matthew Kellway	Beaches East York	ON	NDP	3	
Mrs. Anne-Marie Day	Charlesbourg Haute-Saint-Charles	QC	NDP	2	
Mrs. Carol Hughes	Algoma Manitoulin Kapuskasing	ON	NDP	2	
Mr. Marc-André Morin	Laurentides Labelle	QC	NDP	1	
Mr. Matthew Dubé	Chambly Borduas	QC	NDP	1	
Mr. Peter Julian	Burnaby New Westminster	BC	NDP	1	
Ms. Françoise Boivin	Gatineau	QC	NDP	1	
Ms. Linda Duncan	Edmonton Strathcona	AB	NDP	1	